INSTITUTE FOR NATIONAL STRATEGIC STUDIES
NATIONAL DEFENSE UNIVERSITY

THE MESH AND THE NET

Speculations on Armed Conflict in a Time of Free Silicon

MARTIN C. LIBICKI

The Mesh and The Net

Speculations on Armed Conflict in a Time of Free Silicon

Martin C. Libicki

August 1995
(2nd Printing)

Center for Advanced Concepts and Technology
Institute for National Strategic Studies

NATIONAL DEFENSE UNIVERSITY

NATIONAL DEFENSE UNIVERSITY
♦*President:* Lieutenant General Ervin J. Rokke
♦*Vice President:* Ambassador William G. Walker

INSTITUTE FOR NATIONAL STRATEGIC STUDIES
♦*Director:* Hans Binnendijk

CENTER FOR ADVANCED CONCEPTS AND TECHNOLOGY
♦*Director:* David Alberts

Martin C. Libicki is a Senior Fellow, Institute for National Strategic Studies, where he specializes in the application of information technology to national security and other worldscale applications.

From time to time, NDU publishes short papers to provoke thought and inform discussion on issues of U.S. national security in the post Cold War era. These papers present current topics related to national security strategy and policy, defense resource management, international affairs, civil-military relations, military technology, and joint, combined, and coalition operations.

2nd Printing. First printed as McNair Paper No. 28, March 1994.
UG485.L53

For sale by the U.S. Government Printing Office
Superintendent of Documents, Mail Stop: SSOP
Washington, DC 20402-9328

ISSN 1071-7552

CONTENTS

Terms

Radical change—as the growth of information technology portends—creates a logic which must be grasped on its own terms.

Great change occurs in two ways.

In one, the sleeper awakes to an entirely new world whose methods and mores are so different from custom as to engender the sense of being somewhere abroad. The shock between the future and the present stands as a mighty mountain whose ascent requires arduous and steadfast efforts goaded by the nagging stretch that lies ahead. Many of these changes are sudden, many catastrophic. Adjustment is conscious, and often reactionary—the accidental tourist trying to recreate the comfortable in a sharply changed milieu. It is a tomorrow that is far different from today.

In the other, the sleeper awakes to a world little changed from the one that slipped into the previous night. This new world is comfortable, and easy—or so it seems. Not until some occasion has compelled a look back is it obvious how far one has come and how effortlessly. It is the *past* that is unfamiliar, holding within it, some dim memory of a life that, in retrospect, made little sense—how did one cope? It is a today far different from yesterday.

Given a choice, most would choose the second path of change and, as it so happened, the important changes have been of the second type. Think of a life without the car, the phone, the television, and the machines capable of bridging the vast oceans that kept the rest of the world far from America's shores.

Unfortunately, the second path is also far more dangerous. The world changes, but those in it do not. Never forced to think anew about the implications of change, rarely aware of its pace, people scarcely notice how dysfunctional their assumptions have become. The few who see the future as quite different from the past, and the rest that grow up in the future and have no past, develop assumptions more consistent with the new rules. The rest notice their marginality only if forced to; if the change is gradual enough, man's mortal life span can hide this disjunction within the normal cycles of growth, maturity, and the yielding of place. Barring rigid institutions that mindlessly replicate the reflexes of the past into the future, successive generations can cope.

If the change is steady but rapid, no such optimism is possible. A clash between those who live in the future and those who only think they do because old habits are comfortable will occur within the active lifetimes of both. The consequences of maladjustment cannot be buried in the mortal life-cycle; they must be faced and squarely so.

The challenge of information technology to national security is of that type. Between 1950 and 1980 the number of instructions per second that a dollar could buy doubled every three years; since 1980 the number has doubled every sixteen to twenty months. In the first few years of the 1990s, the pace has, if anything, accelerated. Some slowdown is inevitable, but even at the 1980s rate, a thousandfold improvement can be expected in sixteen years; at earlier rates, a leisurely thirty years. By the time this acceleration runs its course, life and war will have changed radically.

The first reaction of any organization to such crisis—using the classic Chinese definition meaning threat and opportunity—is to absorb new technologies into old ways. So it was with electricity. The electric motor replaced the watermill; the electric trolley, the horse-drawn trolley; television was radio with pictures—and so on. Over time radical changes in technology are understood to involve radical changes in the organization of work and society as well. Initially the electric motor did not help productivity compared to the belt-driven machines it replaced; in time, vertical factories designed to minimize the amount of belting gave way to horizontal factories designed to help the flow of men and material. Similarly, computers cannot help most firms very much until they reengineer their work processes to accord with the silicon logic. Conflict both conventional and unconventional will

perforce follow the same path—accommodating change first by incorporation, and next by reinvention.

No change so large can breathe without metaphors, in this case: Mesh, Net, and Silicon. Mesh—the term applied to military applications—points to the holes; as information technology places a finer mesh atop the battlefield, more objects are caught in it. Net—the term applied to civilian applications—points to the substance of the system; the connectivity of people and their machines suggests new patterns of social relationships and new venues for conflict. Silicon, that which is to become free, stands for both semiconductor chips (for computation) and optical fibers (for communications).

Argument: The relationship of the once and future revolution in information technology to warfare is analyzed in several steps:

- Chapter One outlines the basis for this revolution and explains why its most natural expression is the dispersion rather than accumulation of information power.

- Chapter Two examines its expression on the battlefield in three aspects: Pop-up warfare, the rise of the Mesh, and the evolution of Fire-ant warfare.

- Chapter Three examines whether the revolution on the battlefield translates into a commensurate revolution in military organization.

- Chapter Four discusses implications for acquisition, research and development.

- Chapter Five extends the analysis to the case of low-intensity conflict.

- Chapter Six attempts a broader assessment of how civilian applications of information technology, the Net, may affect national security.

- Chapter Seven contrasts the Mesh, and the Net.

- The Epilogue considers certain reasons why information technology may not translate into the victory of the Small and the Many over the Few and the Large.

1 *The Rising Tidal Wave*

Despite the waning of military technology competition, information technology, driven by burgeoning commercial markets, is likely to continue its rapid pace of development for a decade or two. Such advances are most logically deployed in distributed rather than concentrated form.

The influence of technology on conflict over the next several decades will be the result of a great irony. Just as the political motivation for developing military technology has declined, the information technology fungible to conflict is about to accelerate.

Military Competition Quiescent

The years 1939 to 1989, which included World War II and the Cold War, saw intense technological competition between the United States and its adversaries -- first Nazi Germany and then the Soviet Union. During both Hot and Cold Wars our national security was perceived as directly threatened—any slackening on our part could put us on the wrong side of a deep strategic abyss, with our survival at risk. Our adversaries felt the same hot breath of competition.

Such fears put a premium on developing military technology rapidly lest one side develop an advantage the other could not trump. The strategic arena hosted the nuclear contests, bomber gaps, missile gaps, windows of opportunity and Star Wars. The conventional arena saw submarines vie with ships, tanks with antitank missiles, stealth aircraft with radar-based air defenses, chemical weapons with antidotes and the entire panoply of electronic warfare including counter, and counter-counter. Our advances sparked theirs; theirs sparked ours. Military technology evolved under hothouse conditions, and military equipment became both ever more sophisticated than its commercial counterparts.

The end of the Cold War has retarded military technology competition. Although the United States (and others) may respond with new technology to emergent means of war (e.g., SCUDs used as instruments of terror), no country can respond to our innovations as the Soviets did. Other motivations are also muted. Tomorrow's improved jet fighter may trespass third-world airspace with less loss of life. Yet its successful development would be less likely to influence the global balance of power as preceding developments may have done.

The same trends have, if anything, heightened commercial competition from both former Warsaw Pact technologists, and the growing electronics manufacturing base from a more market-oriented

China. Thus commercial information technology will continue to advance at a rapid clip. With every year, more and more technology comes from the commercial side. Even before the Cold War ended, the leading role of defense acquisition had begun to fade. Military electronics started lagging behind commercial electronics and could only hope to stay current through spin-ons of commercial technologies.

It is precisely as the *motivation* for conducting revolutions in national security technology slows down that the *means* of doing so accelerates. The latter may yet overcome the inertia of the former. At that point, the world of conflict will be radically transformed. Although most elements of the new battlefield will arrive by 2010, exactly when every aspect appears and is demonstrated will depend on who is fighting whom and where. Yet once someone exhibits such capabilities, others will try to follow close behind. Military competition, though usually latent, does not tolerate fudging when it emerges.

The impact of the information revolution in civil affairs is likely to follow a smoother but not less radical pace. Personal computers, networks, facsimile machines, and cellular telephones have rendered large chunks of the West's workspace unrecognizable. Their spread to the South—with its far different societies—is likely to promote even greater discontinuity. In some ways, present conditions in underdeveloped nations resemble past conditions in developed ones: Korea

circa 1988 equals Japan circa 1964. In other ways, undeveloped nations are a synchretic mix of the old and the new. Because Java, Indonesia's core island, is underdeveloped, it should resemble nineteenth century America. Yet three-quarters of all households own color televisions, telephone service is increasingly skipping the wireline phase and jumping straight to cellular, and a coterie of Western-educated technocrats support a highly competitive aircraft industry. It is precisely the combination of traditional mores, rapid urbanization, a lagging overall living standard, but cheap high-technology goods that will make the third world such an interesting stew.

Information Technology Ascendent

Information technology doubles roughly every one and a half to three years. Each successive generation is both faster but cheaper, smaller, and less power-hungry as well. Free silicon is inevitable; more precisely, unlimited amounts of information acquisition, processing, storage, and transmission capability will be available from indefinitely small and inexpensive packages. Limitations on information processing capability will constrain the conduct of neither military and civilian operations. In a narrow sense, ending these limits, to echo Freud, leaves behind all the other constraints in life. In a broader sense, as information gets cheaper, it substitutes for activities that are not information intensive.

Both the breadth and speed of these advances mark the flood. IBM introduced its PC in 1981 based on the Intel 8088 chip running 250,000 instructions per second. Pentium-based PCs introduced in 1993 runs 30,000,000 instructions per second—and for roughly the same cost. The 300 bit per second (bps) modem of 1981 cost more than the 14,400 bps modem of 1993. The IBM PC's original 16K DRAM contrasts with the (slightly more expensive) 16M DRAM expected in 1994. In 1981 the Internet had 213 hosts connected with 56,000 bps digital lines; in 1993, the Internet has more than 1.5 million hosts whose core has 45 million bps digital line today and will have a billion bps lines in two years. The IBM XT of 1983 had a then-enormous 10-megabyte hard disk in a 5 1/4 inch box. Today's choices range from a (much cheaper) 20 megabyte hard disk in a 1 1/2 inch box to a (somewhat more expensive) 600-megabyte disk array in a 3 1/2 inch box. Technologies with no direct precedent in 1981—cellular telephones, compact disks, electron tunneling microscopes, and global positioning systems add fizz to the torrent.

Many observers argue that information technologies will be no exception to the rule that while progress can be rapid for a while, eventually, all such revolutions peter out. For example, every new generation of jet aircraft and engines over a quarter-century period was far more capable than its predecessors. But by the late 1960s only evolutionary change was left; the Phantom F-4 and the Boeing 747

are today still cost-effective for many missions. The rate of new product introductions and market growth for plastics and other petrochemicals was swift in the 1950s and 1960s. (Recall the singular advice, "Plastics" offered to the protagonist of the 1968 film *The Graduate*.) After 1975 both rates declined sharply.

If this theme is generally true, how much oomph does the information technology revolution have? Today's best microprocessors use .5-micron features. One commonly cited barrier to further progress is that feature size can only shrink so much (and thus speed can only rise to fast); this limit, .25 microns, some say will be reached in the late 1990s. Advances below that would require a very expensive transition from optical (and/or ultraviolet) to X-ray lithography or something equally powerful. At even finer geometries, quantum effects may play havoc with any chip howsoever fabricated. Yet these predictions, even if true—and the boundaries below which optical methods fail keep retreating—would not necessarily end the information technology revolution.

First, expensive transitions are not necessarily impossible ones. By the time a transition is needed, industry will have had time to work out and finance new equipment (even if, being expensive, it comes late). Quantum effects, while harmful at one level, can be exploited at another for atomic-level microprocessors.

Second, even assuming a limit on fine geometries, other methods exist to flog the performance of electronics. New chemistries help. Gallium arsenide, whose use is currently inhibited by its fragility, permits the same design to run three to five times faster than one in silicon. The former would also uses less power and can take more radiation. Other electronic materials (e.g., indium antimonide) also hold promise. Performance gains may also come from adding three-dimensional aspects to two-dimensional chips (e.g., trench capacitors or a fully three-dimensional chip). Chip microcode (e.g., RISC, instruction pre-fetching and pipelining) is getting better, which aids all geometries.

Third, better computer architectures multiply the effects of better semiconductors. Massively parallel machines are already in the market; neural networks and good fuzzy-logic chips may soon follow.

Fourth, software is also improving thanks to more efficient algorithms, more reliable programming tools, the compression of image and data, and more efficient coding of radio transmissions. The technologies of artificial intelligence may also start to bear great fruit as well.

Fifth, ancillary technologies are also improving: photonics (a pure photonic computer was bench-scaled in 1992), purer fiber optics for higher bandwidth, magnetic drives down to the size of a matchbox, ever-

denser optical media (e.g., CD-ROMs), the possibility of three-dimensional holographic storage, solid state emitters, and more efficient batteries and solar collectors. Functions that can be transferred from one technology to another will improve system performance even if the technologies themselves have reached a plateau: e.g., switching from slow and power-hungry hard-disk drives to faster and low-power flash memories.

Sixth, not all progress has to be at the leading edge of technology. Steady incremental improvements in the manufacturability of information technology devices spell lower prices which leads to larger economies of scale which spell even lower prices and so on. Since the ubiquity of Mesh and Net is based on the favorable economics of deploying millions of low-cost devices, such improvements make a difference.

Seventh, even if *both* product and process improvements cease, the spread of these devices through normal investment patterns guarantees a continual upgrading of the global information infrastructure.

Eighth, even *after* such an infrastructure reaches a plateau, people will still be finding uses for the infrastructure that they missed seeing.

The accumulation of all these advances sets the stage for continued and probably rapid improvements

in the capabilities of information technology. Maybe the recent doubling times of a year a half will lengthen. Yet were progress to recede to half its rate (e.g., a doubling time of three years) this would merely postpone the revolution; it would not alter its nature.

The Logic of Distributed Intelligence

Most of the recent benefits of information technology are going, not into more powerful computers, but into more widely distributed intelligence. This truism of commercial life can be applied to the battlefield with even greater force. Proliferation in the civil world has its limits—one person can get on but one functioning computer at a time. In the military realm, though, computers could be slaved to sensors and networked. The use of intelligent devices on the battlefield has no theoretical lower limit. Several factors suggest that such distribution is not only possible but optimal.

The first reason is economics. Until the late 1970s, Grosch's law held that doubling the cost of a computer multiplied its power fourfold. Since then, the cost-performance ratio of computers has flipped; it is greater at the lower end than the upper end. Microprocessors deliver more mips (million instructions per second) for the buck than their more sophisticated mainframe or even supercomputer rivals. Even supercomputers, these days, are most cost-effective

when built from thousands of microcomputer or workstation, and the best microprocessors are found, not in giant machines but in workstations, while the most cost-effective microprocessors are in high-end personal computers. If digital television takes off, the most cost-effective chips may be found within these sets, only further validating this generalization.

The cost-effectiveness of employing less sophisticated products manufactured in the millions rather than a handful of very sophisticated products extends to other information products: photographic film, television and computer displays, tape backup (e.g., audio cassette-sized tapes), CD-ROM, and hard-disk drives.

This pattern of the information age stands in direct contrast to historically recognized patterns of the industrial age, where bigger was more cost-effective. For instance, larger submarines tend to be quieter. Full-sized aircraft carriers can launch far more planes yet cost only slightly more than pocket-sized carriers. Heavy space systems can lift a pound into orbit cheaper than their lighter cousins. The Boeing 747 still offers the lowest cost per seat-mile. Auto factories, nuclear plants, oil refineries, cement kilns, and chemical reactors achieved their greatest economies at largest sizes. Exceptions aside (steel mini-mills prosper as their integrated cousins fail; high-capacity fiber optic lines are still the most cost-effective way to send a bit)

information technology tends to be most cost-effective at the low end; industrial technology, at the high end.

The second reason is that distributed systems put intelligence where it can be used. A central box with a hundred phones may offer the most calls per dollar, but forcing everyone to go to the box would be highly inefficient. Even distributing a hundred desktop terminals may be less cost-effective than networked PCs if users cannot customize them and thus avoid using them. One observer has gone so far as to argue that the increase in processing power that PCs brought to the Gulf affected the conflict more than all other computing power combined.

For military operations, efficient area-wide coverage becomes important. A hundred pairs of eyes can always find something in the field most easily if they are spread around rather than bunched up. Dispersion is also good for localizing an object. A hundred low-power noses can detect, and more important, track a scent better than a single high-power nose stuck in one place.

Consider a radar looking for a single intrusion. A single large radar may be more cost-effective in terms of power produced per dollar of installation. Yet the strength of a reflected beam, while proportional to its energy, is inversely proportional to the distance to the object taken to the fourth power. A hundred radars whose maximum distance to the target is ten miles

around will be, collectively, as sensitive as a single radar, ten thousand times more powerful, whose maximum distance to the targets is a hundred miles around. Whether the latter is more economic may depend on other factors. If guarding a radar is the largest expense and all radars need the same complement. a hundred small radars may be far more expensive. Conversely, if the small radars can sit in a common truck trailer while the large radar needs a specialized facility, the former may be more cost-effective.

Third, distributed systems are more robust against accidental failure than large ones. The Capital Beltway can carry more cars than four country roads can, but a single overturned tractor-trailer can close it; four identically timed spills are needed to close the country roads. Two independent units of 90-percent reliability are needed to generate a 99-percent availability of at least a single 100-percent redundant capacity. However, fourteen units of 90-percent reliability will keep at least 10 units on-line 99 percent of the time—only 40-percent redundant capacity. The greater the desired reliability, the greater the advantage of distributing capacity into smaller units. The need for very high reliability can be especially pronounced in a military context. Someone may be willing to wait a year for the opportunities provided during that one hour that the system is down.

Of greater military relevance is that one large item is easier to find than are each of a hundred smaller ones. Small size and large numbers work with each other in this case. First, the one large item usually has a greater signature than *each* of the smaller ones. Second, far more effort is needed to track, hit, and ascertain the destruction of a hundred small ones.

Many vulnerabilities, it remains, are more easily defeated by concentration. The same mass may be enclosed in eight foot-square blocks or one which is two feet on each side; the former require twice the cladding the latter does. Nevertheless, too great an emphasis on defensive measures can lead to self-defeating cycles. The more valuable a single item, the more self-protection it needs, the more expensive it is, and the fewer are made. The fewer are made, the more important each is, thus the more worth destroying, thus the more protection they need and so on. The aircraft carrier carries not only attack aircraft but defensive fighters, electronic warfare jets, antisubmarine helicopters, and air refueling capability. It must sail with an Aegis cruiser, picket frigates, and an escort submarine. Everything but the attack aircraft is designed to ward off and defeat potential air, surface, and subsurface attacks on the carrier battle group. Thus a ten-billion-dollar armada of ships and planes exists to support twenty-four attack aircraft in certain high-threat environments.

Attacks are ruled by countervailing principles as well. After a certain point attackers can saturate even well constructed defenses simply through numbers. Mere confusion (which is rarely so mere) aside, engaging a target takes a certain amount of time, and these sequences often cannot run in parallel. A defender must either take a certain minimum length of time to go through a find-engage-destroy cycle as well as engage an attack from one aspect and then shift to another. Either way, something gets through.

All this information technology will probably not yield robot soldiers. Robots—replete with sensors, silicon brains, and artificial legs—are not impossible. But why must all these be integrated into one package, let alone a man-sized one? Full systems support and integration, if nothing else, is likely to yield a very expensive bionic form, far less capable a network of cheap objects suitably dispersed.

Coordination-and-Convergence

Replacing complex systems with networks of dispersed computers and communications introduces the problem of a complex command-and-control overlay (in civilian terms: coordination-and-convergence). If one head must guide dispersed fingers, both the head and the nerves out to the fingers are vulnerable. Conversely if the functions of a complex distributed system are meted out to various components—each of which must

work correctly—the difficulty of ensuring that *each* component works rises far faster than the total number of components does.

Within the last five years, considerable theory has been done on architectures of loosely coupled processors. In many ways such systems possess considerable advantages over tightly coupled ones.

Neural net architectures—used for pattern recognition—form one archetype. Although neural nets are densely hierarchical—information flows up to a central determination point—they are highly robust. Both sensors and intermediate nodes work without central logic. For pattern recognition, each sensor sees part of a picture, forms a sub-judgment on it, sends a signal to intermediate nodes, which weigh the inputs from sensors and other intermediate nodes, and pass it forward for comprehensive assessments. Matching guesses to outcomes sends grades down the line to each note, subnode and sensor so they can retune their sensing and weighting signals accordingly. Altogether the core does very little work. The system degrades gracefully rather than catastrophically as sensors and sub-nodes go down.

Other models of complex systems built from simple relationships come from self-organizing systems and complexity theory. The former is based on cell differentiation. Multi-cellular creatures such as humans start from a single cell that gives rise to hundreds of

types of cells through genetic sequences that can switch other genetic sequences on and off. Such n-fold complexity requires many simple triggers. The latter suggests that very complicated systems can be created from simple homogenous parts if they interact with their neighbors according to a well-tuned pattern. Tuning matters; outside stimuli sometimes produce no reaction and at other times make the system oscillate to death. Analogously, some people form fixed ideas and never take anything new on board; others react only to new notions and are slaves to trends. Some intermediate method of integrating information can be very efficient at responding to the outside world—even though no individual piece is.

Another, quite different concept is evolutionary programming. Instead of developing a complex optimized program to handle difficult problems, start with a million programs each of whose modules are chosen from a certain set (as a Chinese menu might yield thousands of dinner combinations). Each such program attacks the problem; those who do well survive and start mating (swapping modules) with other successful programs to produce multiple offspring. Eventually, good programs predominate and bad ones die.

These models suggest how systems composed of loosely coupled components can, properly tuned—and there is a world of sophistication to be tapped—survive

degradation, exhibit complex behavior, and learn from external stimuli.

There Will be Other Changes

To be sure, tomorrow's world will differ from today's in dimensions unrelated to information technology. Other technologies will advance—some in ways which may surprise us. Biotechnology, in particular, may go wondrously right or fearfully wrong. Some differences will stem from forces unrelated to technology. Many are negative. Population will grow and mostly in the South, some large share of which will attempt entry into the West. While most regions get richer, some will get poorer. Pockets of preservation aside, the world's ecology will deteriorate—although how catastrophically is unknown. Resources will be depleted and garbage piles will grow.

Yet, the most powerful *predictable* difference is likely to take place through information technology. Vast improvements in information technology are happening now, and will continue to happen; that these improvements will change the conduct and context of national security is virtually certain. Other technologies do not seem to offer as much in the way of change these days and thus do not offer large cumulative advances of deep significance. Technologies that alter society radically—the automobile, modern medicine, precision warfare, and, yes, phones and

computers—tend to result from a long chain of small discoveries and incremental improvements. Future revolutions should have a visible tail today; predicted revolutions that lack a tail will probably not amount to much even several decades hence.

Although material progress does not itself change society so much by itself, it does permit new forms of wealth, power, and social organization. Such opportunities will be seized on by those seeking advantage. Those otherwise disinclined to risk unpredictable changes will be forced to respond. The automobile was not invented to alter the shape of America's cities or the conduct of adolescent mating rituals—but it did so just the same. The radio, in the hands of charismatic thugs, fomented wars. Future changes in information technology will as certainly rewrite the assumptions—both political, and military—upon which national security rests.

2 *The Small and the Many*

Freer silicon, which portends the ability to collect enormous quantities of data, will alter war in several stages. Pop-up warfare describes the battlefield in which the means of war are quiet or hidden until they rise and engage. The growing and (for the time being) unchallenged ability of U.S. forces to lay a Mesh over the battlefield permits the tracking and targeting of increasingly small, quick, stealthy, and transient objects. The logical consequence of this capability's spread is Fire-ant warfare, a battlefield dominated by scads of sensors, emitters, and microprojectiles.

Today, platforms rule the battlefield. In time, however, the large, the complex, and the few will have to yield to the small and the many. Systems composed of millions of sensors, emitters, microbots and miniprojectiles, will, in concert, be able to detect, track, target, and land a weapon on any military object large enough to carry a human. The advantage of the small and the many will not occur overnight everywhere; tipping points will occur at different times in various arenas. They will be visible only in retrospect.

The triumph of the small and the many, of information technologies over industrial technologies,

pop-up warfare, is the expression of 1990's technology under the no-longer-valid assumption that the U.S. faces an enemy with comparable capabilities. The second, the Mesh, describes how U.S. military power (using technologies available over the next twenty years) might work against a foe with developed industrial but underdeveloped informational capabilities. The third, fire-ant warfare, assumes expensive sensors will themselves be vulnerable and have to give way to networks of inexpensive information elements.

Pop-Up Warfare

A tilt toward quality in the quality-quantity equation is a good sign that a military technical revolution has occurred. During the run-up to the Gulf War, Allied and Iraqi counts—manpower, tanks and aircraft—were anxiously compared. War quickly made clear that the Iraqis could have fielded two or perhaps five times as many men, tanks, and planes without affecting the outcome much. Allied technology—both equipment and our sophistication at using it—was so superior (for the terrain) that exchange ratios were overwhelmingly in its favor. We could see and they could not. We could sneak up unnoticed and catch them by surprise. Our weapons could be precisely aimed while theirs were effective only against targets several miles wide (e.g., Tel-Aviv). We were on one side of a revolution and they were on the other.

Yet consider how differently we would have had to operate if they had had but a fraction of our capabilities (alternatively, what a conventional war against the Soviets in the 1990s would have looked like). Virtually everything we used on the battlefield would have been vulnerable had it been visible. We would have had to harden or hide our logistics dumps and command and control nodes. Our tanks, were they are to survive, would have to be hard to find except during those few moments spent scurrying or shooting. Surface ships would have been nearly useless anywhere near shore. Both sides would have been driven to pop-up warfare—a mode in which elements are hidden and quiet except during those brief and dangerous moments of engagement or movement.

Among the various elements setting the stage for pop-up warfare, the precision guided munition (PGM) has probably been the most salient. With PGMs, any locatable object can be precisely targeted and, most likely, destroyed. Any object with a fixed latitude and longitude could be targeted (with cheap, accurate aiming systems) and struck. To do this, today's PGMs use complex homing and terrain-matching devices coupled with accurate gyroscopes and accelerometers. Tomorrow's will be helped by GPS-guided seekers. External systems would relay the latitude, longitude, and altitude of the target, then the PGM would zip to that point. More sophisticated systems would use real-time updates against relatively slow-moving targets and perhaps even local (or relative) positioning systems for

greater accuracy. Moreover, with new assets in space, and the increasing sophistication of airborne sensors (e.g., AWACS, JSTARS), as well as seaborne sensor packages (e.g., Aegis Cruisers), the number of objects that would fall under target scrutiny would increase as well. Thus would fixed and slow-moving targets fare poorly on a pop-up battlefield.

Pop-up warfare puts a great premium on minimizing one's own signatures (e.g., stealth) and amplifying the enemy's (e.g., the data fusion capabilities of Aegis systems). Both sides would have to stay hidden most of the time, pop up just briefly to move or shoot, and then scurry back into the background. To succeed, forces would quickly have to distinguish threats from decoys and friendlies, determine the threats' location and bearing, fire, and then disguise and eliminate their own signature.

Can large, fixed, above-the-ground targets be defended? Some targets can shoot back against incoming missiles. Capital ships, for instance, are equipped with both anti-missile missiles and close-in weapons systems designed to disable incoming missiles with a hail of lead. Sufficiently valuable fixed sights might be protected by upgrades of the Patriot missile, or follow-on versions such as Erint, THAAD, or the Arrow. One proposal calls for hiding anti-SCUD missiles near potential SCUD sights to chase and overcome the latter while in boost phase.

Nevertheless, the betting has to be with the attackers rather than their targets. Targets are bigger than missiles, and missiles shoot first; they can succeed in aggregate by overwhelming the defense with numbers (many of which need only be cheap decoys). Defense against hyperkinetic projectiles could be far more challenging (the SCUD launches into Israel suggest such missiles are even more dangerous after they fall apart). A projectile that reaches Mach 10 or 20 and then releases a shower of darts clad with ceramic (to stay intact under reentry heat) can greatly damage soft targets. If the missile can elude destruction prior to decomposition, mission completion is only a matter of time.

The recent emphasis on knocking out anti-ground missiles in their boost phase suggests the realization that missiles will be very hard to hit once they stop radiating heat. As it is, today's missiles—hard enough to hit as it is—have yet to exploit a deep reservoir of stealth techniques. When they have done so, they will be far harder to hit. The logical consequence of the missile's superior penetration capability is that their targets would have to be dispersed, protected in very hard bunkers, or be moved around all the time.

Pop-up warfare will evolve as signatures can be harvested by unmanned objects: loitering missiles, unmanned drones, unattended submersibles, increasingly sophisticated mines. New techniques of data fusion can help correlated such signatures.

Conversely, platforms will need more stealth to survive. The F-117A, the B-2 and submarines are already stealthy, but stealth is also mooted for missiles, surface ships, and even tanks.

The contest between stealth and anti-stealth will be long and drawn-out, but again the betting has to be against stealth for any platform large enough to encompass a human. A hider must suppress a bit-stream of information that constitutes its signature. A seeker tries to amplify these signals in order to read them. As information technology advances, so does the ability to amplify bits. No such mechanism favors suppression. Indeed, an ecological axiom states that although removing half of a pollution stream is easy, each successive halving is harder. At very low levels, sophisticated devices to clean up one form of pollution often create another. Moreover, the cost of data collection and fusion drops with the cost of silicon. New stealth techniques, although effective, are not getting cheaper.

Thus even with stealth, everything ultimately can be found. All objects have mass and thus gravity. Every object moving in a medium creates vortices and must expend energy to do so. If nothing else, objects of a certain size have to occupy some space for some time. A set of sensors placed sufficiently close together can, in theory, eventually trap everything by getting close enough. A sufficiently fine web can intersect with any submarine. A line of sensitive

receivers placed close enough together will find its line-of-sight path to a beaming object cut if a bomber—no matter how stealthy—rolls past. Neither architecture may be particularly cost-effective. Yet, both show how sensors of certain minimum discrimination placed close enough together can, at some epsilon, catch anything. Hence, the Mesh.

The Mesh

Chances are good that the United States will face a decade or probably two when it can apply military force against opponents with greatly inferior capabilities. Their strategy would not be to defeat American forces in the traditional way so much as to create as many casualties as possible in hopes that the United States would be dissuaded from further pursuit. Our strategy, in turn, is to use our longest suit to control the battlefield to the greatest possible extent to minimize exposure and casualties. As information gathering and processing capabilities continue to improve, our ability to see into the battlefield will increase exponentially. This advance brings with it both great opportunity and problems.

Combat requires doing two things: finding targets and hitting them (while avoiding the same fate). PGMs allow their possessors to hit most anything. Tomorrow's meshes will allow their possessors to find anything worth hitting. Every trend in information

technology favors the ability to collect more and more data about a battlefield, knitting a finer and finer mesh which can catch smaller and stealthier objects.

A long period can be expected in which elements of the Mesh coexist with current platforms. The United States, for instance, will probably be able to deploy fleets of light satellites for surveillance before others can target our existing stock of heavy low-earth orbiters. During that interim the choice of using platforms or the Mesh for any particular mission would depend on which worked better or was more cost-effective. Thus, an initial architecture for the Mesh need not have all capabilities at once as long as platforms to do the same job can survive.

The Mesh, at its outset, would be one part of a cue-and-pinpoint system. Today's airborne sensor system is a multi-layer system of satellites, large aircraft, UAVs, manned aircraft, and finally, PGMs themselves. Under the sea, certain types of sonobuoys detect the presence of submarines by passive sensors, followed by active sensors which localize the submarine by pinging it, followed by torpedoes which use acoustic means to land on top of it. Similarly, the Mesh will be composed of unmanned sensors, infiltrated into existing systems composed of large and expensive platforms. ARPA's Warbreaker project is experimenting with systems that proliferate sensors that allow scanning wide areas for certain types of signatures.

Challenges: Managing the enormous increases in information flow is probably one of the greatest challenges created by the workings of the Mesh. The technical problems—filtering, fusion, and fanning—are daunting enough, but the stickiest ones deal with the distribution of information.

Consider, for instance, a joint task force formed overnight to head off an unexpected incursion in some otherwise forgettable corner of the world. As the crisis starts, the relevant CINC will have a certain flow of information from existing sensors such as satellites, electronic listening posts, and perhaps fielded seismic and acoustic systems. Among his first acts will be to duplicate his enormous monitoring capabilities to some joint task force commander. Shortly thereafter, a new flood of information will come from various data collection platforms such as AWACS, JSTARS, Aegis, and perhaps small satellites and UAVs. Suddenly, the relative trickle of information available to the commander starts to become a current sending forth far more data than any human can deal with. This flow must, in turn, be apportioned to various sector commanders for their action. Atop this flow comes a flood of information as various platforms start to deploy distributed air, water, and ground sensors in various formations. These, too, then have to be analyzed, dissected, and apportioned to the various sub-commanders each of which has a different array of capabilities. Managing such information blooming will require considerable practice.

Opportunities: The development of large effective information collection and analysis systems permits the United States to aid an ally without the commitment of military forces, and in some cases without fingerprints at all. So far, the Soviet Union has provided satellite imagery to Argentina (during the Falklands war), and we did the same for Iraq (fighting Iran) and the Angolan government (fighting UNITA). The denser the overhead information, however, the more help is available. Near real-time imagery of Serbian artillery, for instance, might help Bosnians more accurately target their return fire—information as a real force multiplier.

In times past, the United States has helped allies by providing equipment: examples range from the Lend-Lease program to the provision of Stingers to the Afghan rebels. If these sensors and emitters become global commodities (not necessarily a happy development), the United States could still provide the equivalent of material support. It would silently supply the pattern recognition, data fusion, and command-and-control software that makes these systems function. Bytes leave no fingerprints.

Could demonstrating a Mesh, in detail, induce surrender without the need to use much force? To do so, requires persuading others that the ability to lock onto a platform's precise position is tantamount to ensuring its destruction. After all, the Gulf War allies did not have to shoot down every Iraqi plane to win air

superiority. It sufficed to make a convincing demonstration of "You fly—you die." Such correlation can be delivered through open broadcast (e.g., via one of tomorrow's virtually infinite channels). The potential victim is then given opportunity to demonstrate his distance from the targeted machine. The act of seeing oneself on television futilely trying to hide may be very salutary. Thus might warfare become the child's game of hide-and-go-seek rather than the adult's game of hide-and-go-kill.

Force Sizing: The last implication of the Mesh is that is simplifies what would otherwise be a difficult problem for the United States—sizing the forces. During the Cold War, our forces were sized against those of the Soviet Union; without so large an enemy, the task is far tougher. Force sizing based on war counting (e.g., one-and-a-half wars or win-hold-win) is likely to die a well-deserved death. The use of capabilities-based sizing cannot satisfy for long, either. The capabilities of others are a much better guide to weapons development strategies (where numbers are of limited relevance) than to weapons procurement strategies (where numbers are highly material). To say that military planners should disregard intentions and focus on the strength of others logically leads to a long-run planning goal of an armed forces capable of defeating every one else (including our own allies) in concert.

The rising importance of the Mesh suggests a force-sizing calculus that could be made independent of the precise size of the opposing threat. One precedent is the Navy's rationale for carrier battle groups. The argument was that the Navy needed three carrier groups in every area to keep one on station at all times. Before 1980, the four areas were the Atlantic, the Mediterranean, the eastern Pacific and the western Pacific. In 1980, adding the Indian Ocean suddenly raised requirements from twelve to fifteen. Any debate over the size of the threat (e.g., a putatively aggressive Soviet Union) could be finessed; the number of oceans rather than the size of the threat mattered. Similarly, force planners could start by estimating the establishment needed to deploy, operate, and service the targets generated by a Mesh. Such a Mesh should have minimal coverage everywhere and the ability to go to maximal useful coverage in however many trouble spots we have to simultaneously have to create targeting solutions for. Done right, such calculations should be robust against wide variations in the size and intentions of likely threats.

Fire-Ant Warfare

At some point in the development of the Mesh, our forces will encounter the paradox that those platforms whose capabilities make other platforms vulnerable are themselves vulnerable and ultimately untenable over the battlefield. Our surveillance planes, for instance, not only come in highly non-stealthy platforms that do not move too fast, but they radiate like Christmas trees. Future engagements are likely to see even relatively backwards nations target major sensor platforms. Should they prove vulnerable, other ways of restoring their surveillance capabilities will have to be found, failing which, everyone returns to the days of the blind.

As argued above, an equally if not more effective way to weave a Mesh would be from millions of small objects. They are cheap, they can get closer to the target, and they are collectively most robust against deliberate attack. Deploy enough of them, and they are too cheap to kill.

An analogy to robots may better suggest the wisdom of distributing capabilities. People perceive robots as complex objects that, in every successive generation, come closer to resembling man. A new metaphor developed at MIT is that of robots as ants. Each one exhibits certain limited aspects of intelligence: some specialize in avoiding shadows; others, in walking without stumbling; yet others, in

staying away from each other. Smart ants are less powerful than smart robots, but they are small, light, cheap, versatile, and easy to reprogram. Being cheap, they can be built in large numbers.

Battlefield meshes, as such, can be built from millions of sensors, emitters, and sub-nodes dedicated to the task of collecting every interesting signature and assessing its value and location for targeting purposes. Many of these sensors have already appeared, albeit in rudimentary form. In the future, they will be cheaper, more sensitive, and capable, collectively, of receiving signals from the various parts of the electromagnetic spectrum. Some would be optical sensors—perhaps small charge-coupled devices tied to neural net processors; they could cover not only the visible range, but also near-ultraviolet, and all shades of infrared. Others would act like small radar detectors, either singly, or in computational harmony with its like-minded neighbors. Chemical sensors could detect the passage of machines or their men. Some would sense changes in magnetism, air pressure, sounds, vibration, or even gravity, and so on.

Why this proliferation of sensor types? The easy answer is that warfighting conditions differ. Some environments (e.g., open desert) and targets (e.g., surface ships) are easy to look at; other environments and targets are tougher. To detect the latter may require exploiting the inherent differences between machinery and background which register on other

senses. The hard answer is that single-sensor surveillance gives the target a single-dimension problem to solve. Tanks strive to be hard to see and thus employ camouflage and night movement. Submarines strive to stay quieter, using size, baffling, and ultra-smooth running machinery. Aircraft are stealthy by controlling their X-band reflections by engineering special shapes and coatings. Multi-sensor surveillance, however, complicates the single-dimensional problem by obviating techniques which dampen emissions of one type at the expense of another; moreover, the multi-dimensional problem they create becomes that much more difficult to solve.

No one sensor need necessarily detect every emanation from a target. The more capabilities a sensor combines, the more expensive it gets. Thus the fewer would be used and the easier each would be to find and kill. Alternatively, specialized, perhaps even single-purpose sensors, can each collect signatures, exchange them with subnodes and *collectively* form a picture of a target in its environment.

The Mesh would also contain cheap disposable emitters to illuminate targets with reflected radio waves, generate confusing signatures, and broadcast local positioning signals for precise targeting. Although accurate positioning systems are critical for the operation of a Mesh, full GPS capability need not be ubiquitous (GPS can also be jammed). Emitters that know where they sit and can broadcast relative

distances to the other elements of the Mesh may suffice.

Some sensors may be equipped to move; they may have little cilia-like feet on land, fins in the water, and an airfoil (see below) in the air. Mobility would help right errantly laid sensors, take high ground (trees, houses, hills) in appropriate terrain, and cluster to where other cuing systems suggest the presence of target-rich environments. Movable sensors fitted with precise chemicals or explosives (e.g., for taking out a critical piece of electronics) could be the killing mechanism in some cases.

Perhaps the prototypical sensor would be a sandwich the size of a penny. On top would sit a photovoltaic energy source or optical sensors; next would be a sliver of microprocessor, perhaps a chemical or acoustic sensor, and then a penny-sized battery, a transmitter for an antenna jutting out to the side, and finally some anchoring pod on the bottom. Another design would make the sensor look like a weed plant of a meter or two length. The shaft would be the antenna; the head a spectral sensor device capable of seeing as far as a human can, and the roots would be acoustic and vibration sensors, as well as anchors. To use yet another analogy, sensors might be the size of bottle caps; emitters, the size of soda straws; and miniprojectiles the size of coke bottles.

Architectures: The transition from single source sensors to distributed sensors has architectural implications that will take some getting used to. For instance, most radars today couple a relatively cheap emitter with a relatively expensive collector. Anti-radar missiles home in on the emitter and by so doing and destroy the collector. Distributed architectures would require far more computation to translate the reflections into objects, but proliferating emitters and spreading them far from collectors complicates the targeting problem of the anti-radiation missile immensely. Emitters would survive longer and receivers would remain unscathed. When later generations of missiles learn to recognize receivers by their shape, the latter themselves could be distributed among smaller networked patches. Again, the computational requirements of putting together a big picture increase, but the cost of computation are continuing to decline.

Another advantage of distributing sensors both over space and by type is that it complicates countermeasures. An aircraft pursued by a missile knows it is being tracked, in effect, by only one sensor, and, more likely than not, in only one frequency. Thus dispersed flares, even though they travel far slower than planes, can be picked up as aircraft by IR missiles, which can recognize the bearing of a signal but not its distance (and thus speed). Tracking a plane using multiple sensors requires that the countermeasures exhibit the same three-dimensional behavior as aircraft do; using multiple sensors also requires all

countermeasures to stay together rather than just appear aligned by the perspective of the missile (e.g., the flare, the jammer, and the chaff have to travel together). This is a far more complex undertaking.

Another feature of the Mesh is that it has the capability to replace man-to-man coverage of a battlefield with zone coverage. The pursuit of a given target, which is to say, its signature, need not be performed by chasing it. Instead the overall Mesh can selectively pay attention to zones over which the target is running. It tunes into successive sub-meshes by expanding the latter's communications bandwidth and triggering external sensors to concentrate on an area. This shift has more than metaphorical significance; it also alters one of the rationales of maneuver warfare. The latter has always assumed that being there at the right part of the battlefield was paramount. But being there is not necessarily a prerequisite to seeing there, and not necessarily a prerequisite to hitting there if the range set of one's own weapons is sufficiently dense.

The last idea suggests the eventual waning of a currently popular theme in Army doctrine (first the Soviet's and now ours)—the use of overwhelming force as a psychological disruption at the outset of an operation. This technique may not work as well as expected against a sufficiently well architectured Mesh. One necessary feature in a Mesh is a sufficiently high degree of disaggregation so that the difference between engaging targets all at once or one at a time is

relatively minor. The second feature is at least some practiced capability for graceful degradation so that a percentage loss of capability does not mean a total loss of effectiveness. The ideal is a Mesh that has no center of gravity and thus must be defeated in detail.

Tips of the Spear: Finding targets is one thing, but ending their useful life takes more than bytes. Tomorrow's weapons would likely resemble today's PGMs. Evolutionary improvements in energy chemicals suggest that the warheads and engines could be somewhat smaller but probably not so small as to be radically different creatures.

One big change would be increased use of weapons that do not have to be borne on manned platforms; mines are a good example. Radio contact with the weapon and external cuing systems for its launch would allow the weapon to be positioned closer to its potential targets without putting platforms in harm's way. Thus a battlefield can be seeded with air-dropped munitions which can be raised, oriented, and activated on command.

A second big change would be in the logic of the seeker—or what is left of it. Today's PGMs have to find targets on their own. Sometimes they get external help (reflected laser tags or radar waves); sometimes their path is pre-programmed (e.g., cruise missiles); sometimes they have to take advantage of passive measures such as heat signatures or pattern recognition.

In any case, they have a nontrivial computation to perform. Up to 90 percent of a PGM's cost is in the guidance and control, and most of that is in the guidance.

PGMs operating in a sensor mesh, however, can use the latter's intelligence. A PGM that is given a target's exactly location can get there on its own in many ways. If GPS is jammed, it can use local positioning signals. If it knows where it starts from, its own gyroscopes and accelerometers will tell it where it is going. A purely ballistic flight path may work against slower targets. Others might simply home in on a sensor attached to the target. A PGM that needs less processing can use a simpler guidance system. Thus cheaper, it can be made in greater numbers and can defeat heavily defended targets by saturating them with multiple incoming warheads.

Logistics, Command and Control: The capabilities of even the most elegant military systems are useless without reasonable solutions to the problems of getting them there and talking to them when they arrive.

Getting Mesh components to where they are needed is a problem whose solution will depend on both circumstances and the architecture of the system employed. A platform to insert Mesh parts is a target no less than the platforms the Mesh was designed to fight against. Parts which are hardened can be dropped from air—even from space—or launched by artillery.

Sometimes, special forces could distribute them into very small but critical areas. Micro-motors might even, at some point, allow them to walk into theater (but at no small demands on energy systems) or even drift into theater. Submarines and stealthy surface vessels may be able to lay down a naval Mesh. All these creatures can be also delivered by civilian means. A Mesh intended as a defensive field inside one's borders can be deployed as a mine field might be—except that by separating the triggers (the sensors) from the explosives (the PGMs), both are far harder to detect).

Although command-and-control functions are integral to the Mesh's operation, because a Mesh sees no distinction between communications and operations, the two functions are integral rather than having the first overlaid atop the second.

The more information the sensors collect, the less they need send to a central collection point. Radio spectrum is limited (at the megahertz range; gigahertz spectrum is more available but requires more energy to tap) and battery life is precious. A high-definition video image of a scene (which is still far less than a human eye can see) requires 800 megahertz in raw form, and even 20 megahertz in compressed form. Audio input is continuous and also data-intensive. Only anomalies could be reported.

The challenge of distributed sensors is to identify an object by using disaggregated readings. Like neural

nets, any such meshes would have to depend on a hierarchy of filtering and analysis. Some readings would be matched against pre-determined patterns. This matching requires that each sensor be able to make partial sense of a partial reading, and that these partial readings can be knit into a probabilistic assessment.

The route between sensing and determination is bound to be complicated. Some sensors—e.g., a particularly good eye—might determine a target on its own, but that would be the exception (if nothing else, two eyes are needed to perceive depth for absolute location). Many identifications will be probabilistic based on, say, sightings, heat signatures, sounds, and perhaps chemical emanations. This faculty will be critical when the other employs decoys—not everything that appears to be a tank actually is one. Because battlefields will always feature new and different objects, sensor processors will have to be capable of some level of logic abstraction. Humans, as multi-sensor creatures, are for that reason very good at identifying objects. However, there is no inherent reason to pack two eyes, two ears, and a nose on every sensor if these functions can be distributed amongst many of them. (Perhaps one needs a hundred eyes as often as one needs ten ears or one nose.)

To coordinate, sensors each would have to talk to one another; their activities would have to respond to what others sense (comparable to moving eyes to

follow something). Some of these sensors would have to act primarily as nodal processors, collecting information from other sensors to assess a pattern. These too would have to be proliferated to assured robustness; even higher level nodal functions would, in turn, be scattered throughout the battlefield in lesser densities, and so on down to those communicating directly to humans, off-site coordinators, and/or fire control units.

A key coordination problem among sensors is how to identify themselves upon disbursement. Each must indicate where it has landed, how well it is functioning, and who it is near (and thus will be talking to). Many sensors will die on arrival; others may be incapacitated by virtue of their poor placement. Inevitable gaps in coverage will require that sensors be added, moved around, or converted from one type to another (e.g., we have enough sensors listening to this, listen to that instead). Constant communications would then be needed to determine which sensors still work, which are silent, and which are phony (digital signature can prevent spoofing but requires that sensors know who their neighbors are). Such communications also would indicate where more coverage is needed.

Vulnerabilities: The most prominent vulnerability of a distributed Mesh is that the links among sensors, emitters, and microprojectiles are key to its operation. Unlike complex platforms which couple their various capabilities internally, capabilities of the Mesh are

coupled externally; thus they may be disrupted by what the Soviets called "radio-electronic warfare."

Sensor broadcasts can, in theory, be jammed or faked, just as those from platforms can. Yet, doing so may be harder than it looks. Jamming requires knowing exactly which frequencies are being used, but more important, where signals are coming from. Today's jammers tend to disrupt a signal from one point to another operating in support of a mission (e.g., confound reflections from a large radar meant to be bounced off an incoming bomber). With proliferated sensors, the only effective jamming technique would be to overpower radio signals by jamming continuously in all directions. This technique requires considerable energy—a fact that makes a jammer a highly visible target itself. Besides taking advantage of existing techniques to avoid jamming—frequency hopping, spread spectrum, extreme directionality—the Mesh might also use laser communications, acoustic means, hopping on enemy frequencies, or just not communicating for long periods of time. Indeed, frequent among Mesh communications might be the repeated admonishment to stay quiet for a while because the enemy is trying to smoke you out. Thus, no one could be really sure that all emitting elements in would be silenced (or just waiting for the right time to turn on).

Faking the broadcast of a digital emitter is even more difficult. By broadcasting a digital signature, a

sensor can simultaneously ascertain that the message is actually coming from the sensor, and that the message received was actually that which was broadcast. (Corrupted messages would be internally inconsistent.) This technique requires that each broadcasting sensor have a unique signature and that each receiving sensor memorize the signature of each broadcasting sensor—this is a memory burden, but one which becomes easier with every passing year. Moreover, techniques that allow a communicator to sign a message also permit them to send out false messages knowing that they will be ignored but hoping the enemy will, if not listen, then at least waste power jamming on a frequency not being used.

Platforms Against Fire-Ants

The fate of platforms can be illustrated by examining how they might fare against fire-ant elements.

Tanks: Consider the tank as it rolls over terrain littered with sensors and emitters backed by hidden microprojectiles. Such sensors may have arrived hours earlier or they may lie buried for years awaiting a wake-up call. Sensors to search for large ground objects need not be located on the ground. Much of the load may be carried by drones that can broadcast more information than today's models, stay aloft longer, operate more stealthily, and cost less. If costs get

enough attention, the deployment of many good drones will be preferred to a few great ones.

An unfriendly tank passing by sensor fields could be brought down in several ways. The most direct solution, if available, is to broadcast the tank's location in real-time to an external missile (or some other fire-control solution). Sensors may also be rigged to take a more direct role. A sensor, for instance, that rides atop a passing tank (much as fleas on passing dogs) can serve as a homing device for an anti-tank round. Of course, it must work quickly before it is detected by the tank's smart skin and removed. Sensors may amble over to a tank's vulnerable parts, then kill it by eating its way through gaskets, fuzing moveable parts (e.g., a powdered aluminum-magnesium burst), befouling its air supply, jamming its electronics, smearing its optics, and so on. The latter methods may well evolve from current research on non-lethal warfare. To wit, the chemicals required to stop a tank without killing its crew may be far more compact and thus efficient than those required to blow it up.

Planes: Today's aircraft are optimized—at great expense—to win one-on-one (or one-on-not-too-many) duels against other aircraft and anti-aircraft ground units. The fate of fifty million dollars' worth of aircraft (roughly one) contesting fifty million dollars' worth of loitering sensors, emitters, micro-projectiles may be far less satisfying.

An air-borne sensor screen might contain thousands of nasty objects that may collectively cue firing units in real-time by announcing a target's location and bearing, illuminating it with spattered chemicals, or by bouncing radar on it. Alternatively, if such objects exploded a rain of carbon fibers or ceramic shards, they could take down the aircraft's engines on their own.

Although current technologies do not allow objects to loiter in the air very cheaply (helium balloons aside), today's drones can stay aloft for two weeks. A typical floater may, in a few decades, be the size and shape of a handkerchief, powered by a coat of photovoltaic paint, and girded by a semi-rigid skeleton acting as both antenna and air-sail. Its sensors and processors, no larger than fingernails, would allow it to sense wind movements and configure itself to bob up and down accordingly. Upon detecting hostile aircraft, it so signals to fire-control units or tries to get itself and thousands of its friends to find their way softly into the aircrafts' engines. To friendly aircraft, it sends what it knows about the not-so-friendly skies and otherwise gets out of its way. These floaters need not be stealthy; when deployed in the millions, they will simply be beyond the capability of anything to shoot down.

Ships: The same problem of coping with scads of hostile objects would also bedevil ships and submarines. The elements of a Naval mesh are

presaged by sonobuoys—cheap sensors routinely produced in the hundreds of thousands today. Lower power requirements, more efficient batteries, and perhaps tethered photo-voltaic collectors will give future versions longer lives. They will also be able to sense better, process more information themselves, and communicate both with their peers (vice overhead aircraft) and associated floating torpedoes. They may even be armed and could maneuver to where ships are most vulnerable. Anti-submarine aircraft squadrons will be used only for initial distribution. If sonobuoys can loiter for years until activated, a much smaller fleet of them could handled even this task.

Naval meshes might be supported by fleets of robotic submersibles—perhaps just very large torpedoes—that can chase fast or stealthy targets into heavily mined waters. To protect themselves, ships and submarines would have to physically sweep large stretches of sea before them. They may need a layered net swept fore and aft to a distance of several miles. This would slow them down considerably and reduce their efficacy in a power projection role.

Space: Tomorrow's space forces will combine very high earth orbiters with large fleets of very low earth orbiters. Their tasks will, however, be the same ones they carry out today: communications, observation, navigation.

One shift will be from strategic to tactical uses of surveillance (already being developed in the TENCAP program). To support targeting and treaty compliance, strategic surveillance needs very detailed pictures (e.g., 10 cm resolution) of compact spaces looking for installations that rarely move. Tactical surveillance, although it can use the detail, needs more real-time information. Coverage also needs to be wider because, in a typical tactical scenario (e.g., Bosnia) the field of action is not fixed; it can move quickly and unpredictably. Today's needs for wide-area coverage—looking for certain high-energy events like the launch of a SCUD missile, for example—are met by large satellites in geosynchronous orbit. At forty thousand kilometers up, such orbiters are usually too distant to localize such events precisely. Tactical operations need much denser coverage, and probably from much closer.

Large earth orbiters are also vulnerable to anti-satellite systems no better than those the United States demonstrated off the wings of an F-15 in the middle 1980s. Eventually, large earth orbiters will prove nearly impossible to hide because they are hard to camouflage against an earth background. Since every one must cross the equator fifteen times a day, constant searching can be confined to a small equatorial band. From a higher equatorial orbit, precise optics coupled with powerful on-board processing would make a first sighting inevitable. The movement of satellites, once spotted, can be predicted with great accuracy.

Satellites that use energy to jerk into unpredictable orbits would emit characteristic energy plumes that would instantly cue seekers to the orbital path. Under such circumstances, a spacecraft would be hard put to get more than one or two passes over the battlefield before being targeted and destroyed.

Hence the watchwords will be to fly high (and thus get lost in far vaster reaches) or fly small and dense. The logic of space dominance would require getting the most capability into orbit the fastest and protecting it there against attack the longest. This capability would provide short-term tactical advantages at precisely the right moment. Satellites made small and cheap enough could proliferate and thus make their complete destruction complicated. Surveillance satellites might therefore survive better in the aggregate. Weapons satellites (if not forbidden by current treaties) might not—due to the added size and weight of a platforms required to carry a minimally effective warhead.

Continuous real-time coverage from space would remain unfeasible until satellites become far cheaper. The best look comes from orbiting 400km high (below which atmospheric drag pulls satellites back to earth, and above which complicates the optics problem). From there, a 30- degree field of view to each side yields a 400km swatch but requires 4000 birds (90 birds per each of 45 orbits) to maintain continuous coverage (between the north and south 60-degree

parallels). Affording this fleet within a feasible $20 billion investment budget would require that each bird and shot be less than $5 million. Split 50:50 (assuming $6000 per pound. to low-earth orbit) suggests that each satellite cost less than $2,500,000 and weigh less than 400kg.

The data burden from such a system is big. To picture everything in the world in one meter resolution with 8-bit detail requires roughly 1,500 terabits. If each point is shot once a minute, a total send rate of 3,000 gigabits/second is required. Even with 10:1 image compression and 4000 satellites, each bird must broadcast 600 megabits per second (roughly equivalent to thirty TV signals). Further reduction is possible by sending only the difference between the actual and expected image, although this requires each bird to store 18,000 gigabytes (150 terabits) of image per bird—free silicon in the extreme. If the resolution doubles, the data collected must rise fourfold. Staring satellites can cover known swathes more efficiently, but successful use of the technique assumes the area covered is significantly smaller than Bosnia. Longer revisit times return us to the current system, which is unusable for real-time operations.

Looking up rather than down, denser information technology makes it easier to construct a functioning ballistic missile defense. A dense enough sensor system should be able to track missiles, which must be large (if they are to hold nuclear weapons) and fly

against a fairly clear background. Destroying the missile once it is found, is considered the lesser half of the problem.

Broader Implications

By changing the conduct of war, the Mesh changes its nature as well. It raises serious questions about human command, affects the pace of conflict, and blurs the distinction between civilian and military on the battlefield.

Human Control: Current leitmotifs of information warfare suggest that because militaries possess a command core linked to field armies by command and control networks, killing the core leads to cheap victory. Yet advances in information technologies may mean that the core need not sit in any one location. Teleconferencing, for example, permits a command center to occupy dispersed locations. The core data base can be duplicated in many locations (or can be built as an distributed system to begin with).

Human command would also evolve. Information technology permits greater centralization—because better telecommunications increase the amount of data that can be sent to core. However, it also permits greater decentralization—because better computation allows units to handle more data from colleagues. Tomorrow's military systems will do both.

Headquarters will be able to do more detailed unit control, but units will be able to undertake more functions in degraded communications environments.

Meshes could be engineered to take humans out of many decision loops. Complete removal from the loop is possible. Yet, a technology which *permits* less human oversight need not *compel* it. The bogeyman of an automated war machine will be no greater than it is today. As it is, many existing weapons lack call-back mechanisms. Most mines, for instance, have no man-in-the-loop between detection and explosion. Once a ship's close-in weapons system is turned on, its choice of targets is determined automatically. How different are a strategic ballistic missile that leaves human control once launched and a loitering cruise missile that searches for and destroys a target on its own?

Could fire-ant systems elude human control altogether? Hollywood likes making movies such as *Fail-Safe, Dr. Strangelove, War Games,* and *Terminator 2* that show strategic systems going autonomous. Accidental system autonomy in conventional systems is a lesser problem because they contain multiple decision points and do not have to make all decisions at once. Regardless of how complex the software, the inclusion of enough if-maybe-then-stop locks can limit the risks. An adversary may, however, establish a doomsday ant-mesh system—but these concerns are not new; they

have been familiar grist to nuclear theologists for decades.

In a battlefield in which machines command others, foot soldiers—whose relative ranks have been dwindling for a few hundred years—may be the only humans left. Platforms already dominate low-density environments such as air, sea, plains, and deserts with their ample running room; these platforms, in turn will be supplanted by the Mesh. High-density environments such as cities, jungles, and mountains remain the preserve of the foot soldier; the Mesh will take over much more slowly in such realms. Foot soldiers can still benefit from technology. Helmets, for instance, may house cellular radio receivers, IFFN transponders, video display terminals embedded in pull-down visors, and computers. The latter would coordinate sensor inputs, generate tactical assessments of battlefield conditions, and transmit maps. Passwords or biological makers could ensure that only the owner be able to use them. The individual soldier could thus be made part of the military Mesh (as well as the commercial Net).

The Pace of Conflict: The Mesh may be tomorrow's version of what the Maginot line was supposed to be, a barrier through which no platform can transit without being detected and destroyed. The Maginot line—despite its subsequent reputation—succeeded where it was placed. Unfortunately, because it cost so much to build, France

was unable to finish it, and Germany ran around it to the south. Mesh warfare favors defense. However, unlike the technology of World War I, which also favored the defense, in the next century each side will be able to bombard the other's civilian infrastructure with relative ease. Thus, it will be possible to destroy an opponent's above-the-ground civilization without being able to occupy its territory.

Conflict may then resemble siege warfare—perhaps even mutual siege warfare. The same *cordon sanitaire* technology that can protect a state against invasion can be used by invaders to blockade defenders. Offensive siege operations are a highly unsatisfactory way of going about war for all the usual reasons: they are slow, uncertain, and hurt the powerless while the powerful can claim scarce resources for their own ends. Iraq's experience after the Gulf War is a good example. Long-term maintenance is also a problem. In the 21st century, how long might technology allow a besieged party to endure a total blockade? Would modern polities have the patience or stomach to maintain sieges over years, as the besieged project pitiful images of their victims? Would technology let the besieger blockade such electronic communications or douse the besieged with messages of panic or despair? If such sieges prove impossible—societies always prove surprisingly resilient against aerial attack—what other techniques would be available to contain aggressors one could not destroy?

Mesh warfare could simultaneously be faster and slower than current conventional warfare. Compared to the several months the United States needed to deploy to the Gulf, a mesh could be laid down in several hours. A heavy lifter could transit over the affected area, dispersing large quantities of sensors, emitters, microbots, and miniprojectiles. Upon landing, they would automatically configure themselves into a coordinated network. Some countries may leave heavy lifters on runways for precisely such contingencies. Perhaps the United States could protect a future Kuwait upon first hearing that it had been invaded, although such a policy would not be an unalloyed plus. The ability to promise quick commitments may deprive decisionmakers of the time needed to contemplate the long-run consequences of such decisions. National leaders could regret not leaving erstwhile allies to their own devices.

If both sides tried to set up meshes at the same time, would the race be destabilizing? Provided both mined inside their borders, setting up a fence might, at worst, compel an opponent to set up its. Often, however, such distinctions are not so pat. One party's fence may include disputed or third-party territory. Many collectors see over boundaries: airborne sensors can enjoy a 300km line of sight; sensitive seismic or acoustic sensors can monitor the entire world. Establishing the space component of the Mesh may also induce conflict particularly if the first up can prevent the second from getting up. World War I was

supposedly accelerated by the competition among various countries to mobilize their troops at the border before the other side could. Once the trains, with their rigid timetables, started moving, momentum moved with them to war.

While a Mesh may be built quickly, its operation may retard war considerably. A recent RAND study argued that a squadron of B-2 bombers could destroy an invading armored column in the open. Knowing this, what country would be foolish enough to afford us such opportunity? Instead, unless an invasion could be completed in a few hours, a conventional invasion force opposing a high-information opponent would want to do so very gingerly, with methods similar to those submarine warfare. The Achilles heel in any information system is the extent to which it can be spoofed—a constant throughout military history. An effective strategy would have to combine false negatives (sneaking through untouched) and false positives (decoys). Some methods work better than others. To find a tank requires looking for a correlation among as many parameters as possible. Yet finders must be flexible to see that if something looks like a tank, walks like a tank, quacks like a tank, but does not smell like a tank, it may nevertheless be a tank. Conversely, a decoy does not have to simulate a tank in every respect to be classified as one—just in all features considered important by the other side. It may require many decoys to find which parameters the opposing software deems important and thus uses for

target identification. All this assumes, of course, that in an attrition conflict one can trade decoys for missiles and still emerge on top. Conversely, a Mesh may let a few tanks by to hide its true parameters. For these reasons, the offense will want to move very slowly while searching for weak spots in the system.

Another technique may take advantage of the fact that the ability to transmit information among many of the nodes may be limited by the small amount of spectrum they each have. Thus a strategy of flooding certain nodes with information may degrade the system. In a poorly engineered system, relevant signature information will be randomly dropped. Even in the best engineered system, concentrating on the important data will force the less highly ranked but still threat-defining data flows to be dropped. Either way, the defense deteriorates. However, determining the information architecture of the other side's Mesh to know exactly where it is weak is anything but easy.

It is not clear how one side's Mesh would combat another side's Mesh. Most sensors and miniprojectiles would not only be small, and at least partially buried, but quiet as well; they would be listening much and transmitting rarely. Might hunter-killer microbots be developed to search out and destroy their opposing numbers? Both the difficulty of the likely terrain and their slow speed suggest that such an effort would be extremely drawn out. Confirming that an area is safe

is even harder, particularly if the Mesh lets a few items through as a trick.

Economics may also inhibit an ant-on-ant warfare strategy. By virtue of their mobility and additional sensors, hunter-killer ants are bound to be more expensive than their more passive victims. If the hunter-killers have to get close to passive sensors to find them, then a certain percentage of the victims could be mined to blow up upon being jostled by a hunter-killer. At some percentage those employing hunter-killers must expend more resources than they disable. Killing from afar could easily require armament that is more expensive than the individual sensors themselves, and so on.

Civilian as Military: Mesh warfare not only makes it hard to keep platforms alive on the battlefield, but complicates the task of getting them anywhere near it. Logistics assets, notably airlift, sealift, and prepositioned supplies, are among the largest and slowest of military assets. The difficulty of getting there against an opposing Mesh should be of particular concern for the United States and others who help allies by projecting power over large distances.

Because, paradoxically, lift assets are among the most civilianized of military assets, the solution to the lift problem may be to consciously imitate civilian assets until very close to theater. A ship used to carry war material for West Island would be indistinguishable

from one used to carry commerce to East Island. At some point its destination would be obvious, but by then, it might have already passed its load of sensors and emitters to where needed. East Island could counter this strategy by explicitly granting a digital signature to specific ships, planes, and messages it selects for its own trade. It is not clear whether other nations would cooperate in setting up an IFFN tracking system with a nation that attacks world commerce. Otherwise, East Island would have difficulty isolating West Island from military help without isolating itself from the commercial world it was increasingly networked to.

Wars are not just contests. Removing all platforms—and thus those who man them—from the field of war would not make war safe for everyone, but the opposite. If Meshes promote siege warfare or the civilianizing of military assets, then the distinction between military and civilian erodes to the great detriment of the latter—a reminder, again, that not every advance in the art of war is tantamount to an advance in civilization.

Conclusions

Regardless of how the many implications of pop-up warfare, fire-ant warfare or the Mesh play out, one conclusion is inescapable. The days of the platform as the king of the battlefield are drawing nigh. With its

eventual demise comes a similar demise of organizations built around such platforms and the systems used in acquiring them. To these, the essay now turns.

3 *Toward an Information Corps*[*]

> Technology, used correctly, begets doctrine; doctrine begets organization. To the extent that tomorrow's military power is defined by expertise at information rather than the application of force, military superiority may flow to those organized for the former task rather than the latter one.

Today's relationship between weaponry and information resembles the relationships among weapons systems and other supporting elements such as command and control, logistics, and personnel. Operations sit atop; all else supports them. Current weapons have accommodated the information revolution by taking advantage of additional data inputs, but the military remains organized around units of force.

This architecture may soon become obsolete. Tomorrow's winners may build their forces around a central information processing core. Such a core would launch information probes into the media of war (that is, into ground, air, sea, or space arenas, or the spectrum *per se*). Multiple sensors under various levels

---

[*]This chapter is an adaptation of an article co-written with Commander James A. Hazlett (USN), "Do We Need an Information Corps?" *Joint Force Quarterly* (Autumn, 1993), **2**, 88-97.

of control would gather, transform, fuse, and harness the returning stream, convert it into threat identification, then fire control solutions, and then ladle results in strategic synchrony directly to fire-control units or indirectly to operators.

The traditional relationship between information and force would be turned on its head. Information would no longer serve units of force. Platforms would become vehicles for transporting sensors and missiles. As fewer sensors ride on platforms and more missiles are delivered from unmanned locations (see the section below) the predominance of global information loops will increase. Thus the relationship between information and weaponry is reversed. Rather than information being a service to the weapon, the weapon is the dispatch mechanism slaved to the Mesh. Units of force would be fire support for information systems.

Changes in organization imply changes in relationships and status. Current military structures are built around legions of operators served by lesser communities, such as information, logistics, engineering, and communications. Although "lesser" is not meant pejoratively, in any unit which combines such disciplines, operators take command. Moreover, although officer career tracks are similar up to a certain level, operators clearly make up a much higher percentage of the Services' top ranks (major generals, rear admirals, and above) than they do of their overall officers corps. In the Air Force, for example, a quarter

of all officers, but over ninety percent of flag officers are fliers. Were information warriors assigned to their own organizations (be they corps, services, or commands), their relationship to the whole would undergo a concomitant and perhaps necessary adjustment.

Rationalizing a Corps

The basic argument for a separate Information Corps and an associated command structure linking operations and intelligence is that it would facilitate effective joint operations, promote the information revolution in warfare, unify the disparate information elements and give them an identity, create a common ethos for information warriors, and provide a unified interface with civilian information infrastructures. It would also provide greater appreciation for the role of information warfare.

Jointness: The farther platforms can see and shoot, the larger their battlespace, and the more service-specific battlespaces intersect with each other. Aircraft of the Navy and Air Force now use the same Air Tasking Order. Data collected by Air Force assets guide Army movements. National sensors alert anti-tactical ballistic missile forces of enemy launches. All the services use the same satellite systems. If nothing else, the sheer rate of growth in the volume and variety of data collected makes the construction of

interoperable, or single, information systems all the more imperative.

The information jointness problem bespeaks an important transition in how wars are fought and the diminished local ties between *seeking* and *shooting*. Today the two usually are closely linked. Although prepped by intelligence reports, a tank must both find and kill the target itself. Yet other forms of warfare have already experienced the separation: strike operations are planned from externally collected data; anti-submarine warfare operations use an elaborate localizing program prior to administering a *coup de grace*. JSTARS and AWACS support an efficient cue-and-pinpointing system. The advent of precision-strike systems that use both absolute and relative positioning (that is, latitude, longitude, bearing, range, course, and speed) is at hand. The growing proliferation of sensor systems implies that the targeting systems of tomorrow must be able to fuse data collected from a wide variety of sources. Such fusion means that seamless interoperability is being demanded for missions ranging from single-shot targeting all the way to situational awareness by CINCs.

To illustrate the value of an integrated perspective consider how a hypothetical Unmanned Aerial Vehicle (UAV) sensor package and might be developed—not only its hardware, but also its software, communications, integration with other data units, and most importantly its doctrine and concept of operations.

The use of UAVs, as all services recognize, can help warfighting. So thinking, each service could develop a package to fit its own mission profiles and support its own platforms. Yet data coming down from UAVs would more logically go to common data receptors and there meld with other joint data collection assets including ground-based sensors, higher-altitude aircraft, and space sensors. To the extent that each sensor package performs its own on-board processing, it may wish to take advantage of common neural training regimens and pattern recognition tools. Data from the various sensor packages—which could come from any of the services—have to be analyzed in real time to determine where follow-on data collection efforts have to be focused, or whether and when fire control solutions have to be generated. The interoperability requirements of such a package are therefore demanding.

The need for interoperable information systems has been widely recognized by the senior leadership within DOD. In 1993, former Secretary of Defense Les Aspin observed in a graduation address at the National Defense University, "Most of our systems for the dissemination of intelligence imagery cannot talk to each other." The principal joint command and control initiative (C^4I for the Warrior) is almost exclusively about interoperability. It mandates that all new information systems must be able to communicate jointly. Unfortunately, history suggests that after-the-

fact standardization frequently leads to unsatisfactory results. Why?

- Standardization is a long-term process that accommodates new developments only after long lags. Over the next twenty years the percentage of new applications to existing ones is apt to grow greatly—intelligent filters that correlate and process multispectral and nonelectromagnetic inputs are on the threshold of major growth. Thus, the ratio of stand-alone data to integrated data will rise unacceptably high.

- Standards developed by competing interests often choose a least-common-denominator approach, letting each side agree to disagree at the expense of interoperability.

- As poor as the prospects for data interoperability are, the growing requirement for software interoperability is even farther from solution.

Returning to the UAV sensor package, development by different platforms groups increases the possibility that each system stands alone, making complete data fusion that much harder to achieve.

An Information Corps is an alternate route to data integration. Instead of having the services and DOD

agencies (and the multiple communities within them) attempt to merge information collection and dissemination systems, the functions would be carried out by a single organization that operates under a unified doctrine and a single command. Data would be standardized from the start; internecine politics that allow components to agree to disagree would be, if not eliminated, then substantially muted. What would otherwise be a conflict between the need for innovation in data collection, and the subsequent need to report only that which has been standardized, would be muted as well. Successful doctrinal innovations would be integrated into the whole much earlier in their development.

A related rationale emerges from the emphasis on Joint Task Forces (JTFs) that are expected to characterize an increasing share of tomorrow's fighting packages. Such organizations usually are made up of a chunk of this and a chunk of that. To work smoothly most chunk commanders (and key staff members) ought to know each other beforehand. A coterie of information warriors whose specialty is preparing the battlefield image but who are attached to different operating units is already integrated. Acting as the glue, they can integrate far more fine-grained units in precisely that area where interoperation is most important: information.

Innovation: Predicting the demise of the platform is far easier than having operators accommodate this

demise. Left to themselves people tend to apply technology in ways which conform to their basic world-view—warriors are no exception. Thus innovations in equipment or doctrine which threaten such an order are likely to be resisted by operators. Granted, no one questions the overwhelming relative superiority of the U.S. Armed Forces, and for that reason our manned platforms would logically be the last to be threatened. However, potential competitors would be foolish to challenge our dominance by a strategy that copied our force structure. Forces built around information systems constructed from commercially available components, however, would pose a more serious threat—one which contests our reigning paradigm. Thus, it would be far more attractive to challenge us.

Although an Information Corps may not be *inherently* more innovative than the Services, it is more likely to pursue the kinds of innovations that accord with the logic of the information revolution. Left to themselves, the Armed Forces will incorporate information into weaponry, but with information technologies as platform support rather than with platforms as fire support to an information mesh. An Information Corps would take an entirely different approach from the outset, emphasizing the information mesh as central. Constituent elements and doctrine for such a mesh would be evaluated on their ability to locate, track, and evaluate objects and events so that they may be passed for conversion into fire-control

solutions and servicing. Such a service or corps would be an institutional advocate for a paradigm shift, and would, by its advocacy, better prepare for a threat which comes from a different direction.

Unity: The common argument against creating a completely new organization is that its planned functions are all being done by someone else. When this issue is raised, however, the composition of the group varies widely: the Director for Command, Control, Communication and Computer Systems (J-6) on the Joint Staff, the Defense Information Systems Agency, the Defense Mapping Agency, the Space Command, and intelligence agencies—all without going into the services. Under the last are specific functions such as command and control, electronic warfare, meteorology, oceanography, automated data processing, and high-information platforms such as Aegis, AWACS, JSTARs, and UAV contingents. Other functions which technology may soon enable are not even listed for obvious reasons; when they do emerge, the soup will be even thicker. This is just the point. The various sub-communities in the information-based warfare community see themselves as disparate players. Each relates to one or two others at most, and they all lack the common unifying doctrine of operations. Information warriors are more than simply communicators, data processors, or intelligence agents. They are all part of a global structure that would become apparent with the creation of an Information Corps.

Culture: A related reason for integrating various DOD informational elements into a single corps is to provide information warriors with status, culture, and an ethic. The issue of respect is relatively straightforward. As information becomes more important, so is cultivating the ability to develop and manipulate it. DOD needs to attract these people not only as contractors but more importantly as operators. Successful military organizations must deploy not only superior information systems, they must also be able to fix, adapt, and maintain them in battle in real time. Yet an aspiring officer today would be advised to specialize not in information but in operations. Even the Air Force—the most information-intensive service—is oriented toward its fighter pilots just as the Navy is to ship and submarine drivers and naval aviators. Top echelons in other specialties such as administration, material management, and command and control are often assigned from the ranks of operators. This procedure makes sense if various specialties call for similar skills and the best are attracted to operations; an elite is an elite regardless of what it does, and it could as easily be mergers and acquisitions. However, if the skills required to be a good information warrior are different from the qualities and ethos needed to be an operator or these skills require long, specialized training, then such logic makes less sense. The best people avoid information; those who remain do not get the consideration their views deserve.

An Information Corps offers the possibility of separate and more appropriate training and career management as well as an ethos for an information warrior. As computers get more sophisticated, training necessary for their effective use gets longer. The information warrior must know not only programming but systems integration and systems theory, communications, electronic combat, security, artificial intelligence, logic in all its many forms (classical, fuzzy, and convergent), and statistical techniques. The information warrior must also know the customer's needs: the commander's intent, doctrine, and strategies. In addition, the information warrior should know something about specific media (land, sea, and space). Sending a college graduate to the field for a few tours of general expertise interspersed with training classes and then expecting first-rate information techniques in a more specialized tour later may not be adequate. The amount of information necessary to be an information warrior is immense, and the time required to master it will have to be at the expense of more general command instruction. If this tradeoff is to be made voluntarily, the results have to be rewarded commensurately. An integrated Information Corps with clear career paths and opportunities for command and success would do this.

As for ethos a divergence between operators and information warriors must be expected. Discipline under fire places a premium on certain qualities: courage, decisionmaking skill under pressure, good

instincts, self-control, loyalty, and so forth. The information warrior, by contrast, must be highly intelligent, creative, independent, flexible, tenacious (to counter infamous 3 a.m. computer bugs) and maybe somewhat eccentric. The example of Admiral Grace Hopper will not excite a tank commander any more than General George Patton excites a bit twiddler. These qualities are not necessarily antithetical, and some qualities—common sense, judgment, contrapuntal thinking, decisiveness—are uniquely common to all warriors regardless of weapons. To seek such qualities in operators and not information warriors further relegates the latter to subordinate status.

Status, ethos, and training issues suggest the need for an Information Corps as well as a unified or specified information Command. Such a Command could produce unity of operation, advocates for change, and liaison, but it takes a Corps to provide doctrine, status, or continuity (e.g., information warriors who are evaluated by other information warriors).

Liaison: In the same way that the information space of the various services converges, so too is the information space of the defense and commercial sectors. DOD uses commercial communications satellites and bought the bulk of Spot's imagery in the Gulf War; boaters use the DOD Global Positioning System. The defense and commercial sectors swap weather data; the DOD Global Grid is the military version of the National Information Infrastructure

(which is a component of a global infrastructure). An Information Corps would play a major role in the development of a national information strategy and a complementary national military information strategy.

As the warning sign to builders "Call Miss Utility Before You Dig" suggests, both communities will have to shake hands before one or the other adds, subtracts, or alters its infrastructures. DOD used to formally liaise with AT&T when the latter was still dominant in telephony in the United States. Since then, the number of information players has multiplied—and not just because AT&T has been rent asunder—the influence of private networks has grown and number of various media has proliferated as well. In addition, as the DOD need for information intensifies, and its assets commingle with commercial systems, the volume of interaction will grow substantially. A common point of contact on the civilian side—with its public and private players—will never happen; a common point of contact on the military side is quite possible. A separate Information Corps would provide not only a common point of contact but common doctrine and outlook. With a national information strategy and a national military information strategy, human protocols would not have to be reestablished every time the two worlds come in contact.

Information Warfare

Just as the land, the sea, and then the air became realms of conflict—and thus called out their own services—so too might information be a realm of conflict, with similar implications. Information war, a clear official definition of which is yet to come, can take on several meanings.

If tanks fight tanks and subs fight subs why shouldn't information corpsmen fight each other? One increasingly popular concept calls for information superiority to be sought before seeking air superiority, which in turn, is a prerequisite to surface superiority. Two sides would duke it out to determine who could control communications on what frequency when, where and under what circumstances. Such conflict would feature jamming, deception, blinding, and firepower against key emitters, sensors, and other nodes. A related notion is for the data warriors to ascertain the other side's command-and-control architecture so that its weak points can be targeted. This would be coupled with the defense of one's own architecture either through a combination of engineering, bulwarking, massive redundancy, message prioritization, operational security, and deception. The relevance of this definition may be limited, though. Technologies such as frequency-hopping, spread-spectrum, and lobe control makes jamming relatively harder. Sophisticated network architectures leading to radical dispersal of command-and-control may

complicate targeting efforts. However, it may take decades for our putative opponents to get such techniques right. In the interim, an information corps would be able to conduct such warfare more efficiently as an integrated team.

Another concept of information warfare posits it as the *only* stage of conflict. An information corps would be the body responsible for developing the doctrine and battle plan for such operations, then carrying them off. The Gulf clearly indicates that a ground force in conventional conflict cannot prevail against an enemy with air supremacy. Thus air supremacy alone may cause the loser to sue for peace prior to ground conflict. By the same token, information supremacy (if such a thing can be defined) may be sufficient harbinger of air supremacy and prompt a loser to sue for peace before a full-fledged air campaign gets underway. Defining such a hiatus before aerial conflict and the preceding information conflict (especially if the latter entails some destruction from the air) may need further refinement.

A related notion is information warfare not as a prelude to but as a substitute for conflict: e.g., non-lethal strategic warfare against key information systems such as air traffic control, space-based commercial communications, and financial networks. The advantages of such conflict for the United States, however, should not be too easily overestimated for three reasons: *One*, as the most sophisticated

information economy, the U.S. is the most vulnerable to such warfare even if it is also most capable of conducting it. *Two,* networks can always be made relatively secure against attack either directly (better, more intrusive security regimes), or via backups that use completely different architectures—like land-line systems as backups to radio-based ones. Improved security costs more, but if network security is prerequisite to national security such price is more likely to be paid. *Three,* it may be far easier to isolate national information systems from international ones (either physically or via revoked permissions) than to make national systems crash. Such isolation, however, assumes that they and not we are hurt more by such barriers. For example, isolating a Chinese-dominated East Asia from the rest of the world may be akin to "fog in channel; Continent cut off."

Finally, the United States may provide information warfare capabilities as its sole or predominant contribution to an effort in which the actual fighting is done by such others as allies, or host nations. This, as noted earlier, has several advantages for the United States. It plays to our strength, minimizes casualties (to which we are becoming increasingly sensitive), eliminates most of the problem of lift (and its interdiction), and grants us at least some plausible deniability for the consequences. One of the strongest rationales for an Information Command is that such a campaign would come far more naturally to some

future information CINC than it would to a regional CINC.

Functions of a Corps

Determining what an Information Corps does (on formation, its duties would be those of the units which comprise it) is tantamount to delineating the borders between the Corps and the services from which it would grow. The first concern is doctrine. The transformation of the Army Air Corps into the Air Force was more than a catch-all for those who flew planes; it was also an expression of a theory of war, to wit: the ability of airpower to transcend the ground situation and transform strategic conflict through aerial bombardment. The Marine Corps has its doctrine of amphibious warfare. Each service maintains its ability to comprehend war from its perspective.

An Information Corps would also have its doctrinal objective: to develop and exploit an integrated image of battlespace. This integrated image would, in turn, be divided and apportioned to meet the needs of various warfighters. Slicing and dicing would entail analysis, filtering, enhancement, correlation, data fusion, and whatever else is required to assist decisionmaking. The image, in turn, is an important component for decisions which range from strategy to weapons control. The bounds of such a system would vary from situation to situation. In some cases a

coherent image would be used for centralized decisionmaking (such as an Air Tasking Order); in other cases the need for a better image would call forth efforts to collect further information (launching sensors). Some fire control solutions would be automatic, to take advantage of evanescent opportunities that a decisionmaking hierarchy would only slow down. Other images are background to on-the-spot decisions (tanks should not have to relay pictures of targets to a central mesh for a go-ahead before engaging them). Clearly the usefulness of a unified image depends on what percentage of the information involved in making a decision is generated by the shooter (coupled with what share of the processing necessary to transform data into decision is supplied by external algorithms). The doctrine is predicated on the assumption that nonlocal information (from other units or remote sensors) and analysis (from artificial intelligence) would rise in relative importance.

Should any operation that involves information, or alternatively command and control in its broadest context be part of a corps? This is probably too broad a sweep. Not only does everyone deal in one respect or another with information, but command and control tends to involve the top level of a hierarchy. To suggest that an Information Corps would become the top-level corps within DOD to which the services must report is presumptuous. To use such a corps to collect, process, transmit, and present information, then convey the resulting orders, however, is not.

At the very least, an Information Corps must encompass those elements which gather, assess, and distribute both silicon- and human-based information: an infosphere. Space would be a central component, since virtually every current use of space (e.g., surveillance, communications, navigation) is directly involved in information. Added to that would be chunks of the intelligence business, and the creation, operation, and maintenance of *fixed-site* command and control assets, information collection systems (such as ground-based radar and SOSUS), mapping, and meteorology, as well as the non-motile elements of the Mesh.

How far should an Information Corps extend into *mobile* information collection? Platforms as diverse as AWACS, JSTARS, AEGIS, P-3 squadrons, unmanned aerial vehicles, artillery trajectory indicators, portable radars, and the like are information-intensive and thus similar to fixed-site information systems; but not every function (like airplane driving) on such platforms is appropriate for the Information Corps. Consider the case of an AEGIS cruiser: it certainly collects a considerable volume of data, and much of it could be transformed into actionable targets for other platforms, but most of its functions call for other skills. Which among equipment maintainers, screen watchers, situation assessors, and communicators should be data corpsmen? Should they be permanently or temporarily assigned?

Such questions lead into difficult issues of scope, or how to prioritize among information flows. The forthcoming information architectures of the 1990s, complex as they seem, are relatively simple compared to what the twenty-first century's will bring. As popularly envisioned within the armed forces, the key function of today's information flows is to enhance the commander's situational awareness by developing an accurate, timely, and correctly detailed battlespace image. This image is devolved to the troops as per their needs. The number of sensors involved in this imagery is relatively small.

With the proliferation of sensors, the task shifts from providing the commander a view of the other side's tank columns, to providing operators a view of the other side's individual tanks. A smaller chunk of information goes to supporting command; more goes to supporting individual units of fire. The unitary view of what gets collected, how it gets collected, and what gets analyzed and presented therefore becomes much more complex.

Who determines this? The level of detail for the top commanders (who have only limited familiarity with the panoply of collection) is too complex for individual determination. The limited scope of sub-commanders (plus the fact that sensors will cross whatever artificial lines are established between them) makes their choice inappropriate. Letting the information commander choose may generate a coherent collection solution, but

whence user input? The natural tendency may be to provide too much collection and information using the same logic that, in health care, is known as defensive medicine. These issues need considerable work.

A tougher question will involve the mix of military and civilians in an Information Corps. Should it be a Defense or Joint organization? Some functions of an information service can be best performed by military personnel with varying degrees of expertise and experience of the weapons systems with which they must interface. Other positions will have to be filled by computer jocks who are not disposed to military service.

Objections to a Corps

The difficulty in delineating an Information Corps suggests that creating one, at least in a platform-centric world, is at least somewhat problematic: it must interface with other command and control organizations, will remove critical functions of an operational unit, and may perhaps relieve some of the pressure of jointness.

Autonomy: Single-service cohorts are generally capable of operating autonomously in tactical environments, with little help needed from the others. Except as noted above, an Information Corps could not. If limited to fixed-site facilities, the Corps could at

least function autonomously, but its value would depend on its ability to provide data to others—it could complete few military missions on its own. But with dispersed sensors and emitters like UAVs, buoys, and listening posts gathering a larger share of the total data, a fixed-site Information Corps would be limited to strategic surveillance and distributed interactive simulations.

Including mobile elements in an Information Corps introduces command problems. Each unit of an Information Corps would have to report through its administrative chain of command, but it would also have to respond to the operational chain of command as well. Who, below the CINC or JTF commander, determines, for instance, when and where to deploy sensors? Who determines whether an aircraft is used for reconnaissance, electronic warfare, strike operations, or emitter dispersion? Do such needs respond to the requirements of the travelling unit (ship) or the deployed units of some information command (or under centralized control if not command)? The time required to resolve these issues or await their eclipse by circumstances (if ships disappear, shipboard problems do also) should not be underestimated.

A related objection is that even platforms whose exclusive mission today is to gather information may not necessarily retain that character. Reconsider UAV sensor packages. If the developers of this hardware and doctrine are information warriors rather than

operators, they may not appreciate the potential of a UAV as a laser designator or a weapon rather than simply as a data collector. Such considerations have to be carefully melded into acquisition process.

Criticality: Every organization is an information organization; moreover, information is power. Removing information cadres from such an organization may promote several unintended consequences. Operational units may be tempted to duplicate their lost capabilities—every important organization in the Federal Government maintains its own policy analysis shop. Besides wasting resources, it reintroduces the very coordination shortfalls an Information Corps was designed to overcome. Alternatively, affected military units may simply ignore the information they cannot control, relying on time-proven but obsolescent means to gathering information (reconnaissance in strength) rather than methods which technology makes more appropriate (sophisticated sensors). Thus, the very modernization that an Information Corps was meant to induce would be retarded by its formation. To avoid this shortcoming, strong leadership would be required inside and outside the corps.

Jointness: Finally, while creating an Information Corps may promote a joint battlespace image, it may retard other aspects of jointness. Removing the most important reason for the services to work together (they would instead liaise with an Information Corps)

removes a large part of the impetus for operational units to work and meet across service lines. The need for joint deployment, joint operations, and, most important, joint thinking, remains, but the day-to-day practice of working jointly would be undercut by the act of shoving off certain joint duties to separate organizations. When the time came to act jointly, the various components would be far less prepared than if they had interacted on a day-to-day basis. The current concept of parallel jointness among peer services may need to be revised to accommodate a Corps that thinks itself superior working with operators who cannot help seeing the Corpsmen in their former support role.

Conclusions

When it comes to radical reorganization—and forming an independent Information Corps certainly qualifies—a first rule of thumb may be: when in doubt, don't. As wars are currently fought, the need for a data corps is, while perhaps inevitable, not necessarily urgent. Unlike, say, the Army Air Corps, which was a single identifiable operational arm, an Information Corps would have to be merged from several disparate organizations. By taking from all services, it would be opposed by all—a resistance difficult to overcome.

The logical conclusion, nevertheless, is that DOD should makes steps to form an Information Corps. The

argument is that a corps would promote jointness where it is critically needed (information interoperability), elevate information as an element of war, develop an information warrior ethos and curriculum, and heighten DOD attention to the global civilian net. When threatened with the loss of personnel and resources, the services may respond that they are doing all of this and more. The greater the threat, the more meaningfully the services may respond. With luck, their response may address problems—integration, doctrine, or ethos—that would otherwise call for an Information Corps. Solving these problems, after all, was the original point. But can they do it as effectively as an Information Corps could?

4 *Wares of War: Hard and Soft*

> Outfitting the Mesh means a shift from few complex items to many simple items knit together by software. For systems acquisition this means building from dual-use parts, fostering open systems, and defining a new role for software.

It is no big secret that today's acquisition system is under stress both from its own dysfunctional internal dynamics and the difficulty of accommodating the post Cold War drawdown. Problems range from very extended cycle times, continuously escalating costs, and excessive overhead, to a technology base that lags commercial developments and has not made an easy transition to commercial conversion. Important questions are being raised on the relative priority of prototyping versus equipping the force, the control of proliferation, and how the industrial base drawdown should be managed in case the United States might need it again.

These discussions tend to overlook how changes in the weapons of warfare may, themselves, affect how the acquisition system ought to be run. Not surprisingly, the optimal method of developing and acquiring elements of the Mesh will, for that reason alone, differ radically from optimal methods of developing and acquiring industrial-age weaponry.

Building Swords from Plowshares

A typical defense system starts life as an operational requirement. This requirement is converted into a basic system design which drives development programs. The design, in turn, is broken down into sub-systems and components. As presently constituted, defense acquisition is predominantly demand-driven. The alternative model, which looks at what is out there and develops innovative ways of using it in defense is far less appreciated. More generally, system designs are only modestly affected by the cost tradeoffs that routinely go into, say, automobile design decisions.

True, this logic is coming under increasing attack on its own merits. Yet, a shift from complex platforms to networks of sensors, emitters, and microprojectiles will (or at least ought to) accelerate the trend to greater cost sensitivity and growing reliance on commercial capabilities in defense acquisition.

One reason that cost competition plays such a small role in major systems issues is that contractors rarely see the sales gains from lowering their own costs. A thirty percent cut, for instance, in the cost of an F-14 carrier fighter is unlikely to result in commensurate increases in the number purchased. Other factors—prior force planning, the logistics infrastructure, the number of pilots, or carrier deck space—put an upper limit on the number of F-14s

acquired. By contrast, the cheaper are the elements of the Mesh, the more densely they can be dispersed, and thus the more capable the overall system. As the elements of the Mesh become less expensive, networked sensors, for instance, can increasingly substitute for large platforms in the same function. The logic of the Mesh, overall, is heavily driven by economics. Indeed critical architectural and operational issues (e.g., what is the proper density of flooding, jamming, spoofing, decoying, and coverage) have to be decided, in large part, on the basis of which side can afford to throw what kind of resources into a thing-on-thing attrition campaign.

As the number of elements in the Mesh runs into the millions, economics will force systems to be designed around technologies already extant in commercial markets, because the latter alone are large enough to offer economies of scale. Even if military items are not, themselves, commercial items, this linkage requires closer attention to using commercial production facilities and practices. What about the counterargument: if acquisition rates are really so high, might not defense procurement alone generate the economies needed? This fails for two reasons. First, the elements of the Mesh are consumables and, in all likelihood, of relatively quick manufacture. DOD would be better off stocking a few months of them and rely on post-crisis production to make up the rest. A commercial base permits a faster ramp-up in emergencies. Second, the culture of commercial

production makes more sense for quantity items than the culture of military production. One reason that defense goods are so expensive is that each is engineered, tested to ensure that every single item has the highest chance of working. The more fussing, the higher the cost; the higher the cost, the greater the urgency of assuring that each works. Elements of the Mesh, however, can do with statistical quality control. Because of how they are likely to be deployed, a certain percentage failure can be assumed. The system, rather than the individual element, is what needs to be configured for reliability—which it does through planned redundancy.

As it is, information technologies, because they perform similar functions whether in military and commercial employment, are already best suited for non-MILSPEC treatment. The few information technologies hitherto thought unique to military needs (e.g., encryption, spread-spectrum, frequency-hopping) are being adapted to commercial users anyway.

For these reasons, the build-or-buy decision for elements of the Mesh can proceed in a progressive winnow. Some capabilities will be available off straight off commercial shelves, and some will need to be modified for military needs. Others could be helped by defense-led efforts to accelerate the development of dual-use items so that they can appear in defense systems at the right time (and under control of U.S. producers). Still others could be developed in

conjunction with new civilian infrastructure projects. The remainder, primarily defense-oriented programs, would represent a reorientation of existing work plus altogether new starts.

Key Technologies: This winnowing can be illustrated by examining the key technologies for the Mesh: electronics, micromechanics, sensors, space, and energy all undergirded with improved manufacturing processes.

Commercial users will drive most *electronic* technologies (notably digital computation, neural-net hardware architectures, parallel processing, and digital signal processors). DOD could help advance non-silicon optical and electronic materials in its usual ARPA-like ways, and support generic advances in manufacturing such as Sematech. DOD is likely to be more independently active in analog areas such as microwave and extra-high frequency communications, emitters, compact antennas, and counter-EMP hardening.

Major advances in *micromechanics* are likely to lag similar advances in electronics by one or two decades. Nevertheless, fields with promise include ultra-light exoskeletons and very small legs, some of which could locomote penny-sized sensors and others which could manipulate a windsail (to support airborne sensors aloft for long periods of time). Some

micromechanical devices may find use in chemical and pressure sensors.

Among *sensors*, visual and near-visual (IR/UV) passive collectors are most important. DoD will probably have to be the primary funding agent for improved sensors. Commercial versions could be spun off to uses such as medical instrumentation, optics, and robotic systems. Similar patterns would prevail for acoustic/pressure sensors, seismic sensors, and various chemical sensors. The latter can find use in medical, agricultural, and environmental fields. Fiber optics is showing promise as a the basis of very fine movement detectors.

The successful use of *space*-based eyes and brains in the mesh is more likely with every drop in the cost of lifting a pound of material into low-earth orbit, and with every method to shrink components found in large spacecraft (power, stabilization, maneuverability, common busses). Ultra-stabilization—to permit satellites to communication down to specific earth collectors—would also improve the ability of space assets to do continuous tactical monitoring as would improve hand-off methods as satellite coverage keeps changing. DoD-sponsored improvements could be shared with NASA (and visa versa), but commercial space activities—unlikely to grow for another decade or two—should not be counted on for much help.

Three *energy* technologies which need further development are batteries, photovoltaics, and remote deliveries of energy infusions. Better batteries would extend the life of sensors, particularly those used underwater. Photovoltaic collectors and energy beam delivery would allow continuous energy feeds in remote locations. Battery and photovoltaic technology (which the Japanese lead us in) have strong commercial applications, and both are consistent with a revitalized interest in renewable energy sources—thus piggyback opportunities. Remote delivery of energy infusions has applications in space, as well.

Manufacturing technology is also critical for its contribution to the affordability that a system composed of many small items needs. Although a specific research agenda must be tailored to specific product lines, two thrusts, miniaturization and more effective cost/quality control, are likely to recur. Any DoD effort to improve manufacturing technologies is best pursued within a consolidated federal thrust and need not be separately programmed.

Civilian Megaprojects: In developing technologies that are needed for the Mesh, DoD may want to look for opportunities to piggyback on top of civilian megaprojects planned for this decade and the next.

One candidate, born Mission to Planet Earth, monitors the earth's environment with low-earth orbiters. The advance of Earth surveillance in general

should support better remote multi-spectral sensing, high-bandwidth data dumps from space, sophisticated software especially for distributed access, and orbiters useful for tactical surveillance in general. A successful National Aerospace Plane could slash per-pound costs to orbit.

The High Performance Computing and Communications program seeks thousand-fold improvements in supercomputer speeds, and very high capacity communications lines—both with Mesh applications. If the program connects schoolrooms to global libraries, it may promote information standards (as a key aspect of systems integration) that could help integrate all those sensors, emitters and nodal processors in the Mesh.

Another program, Intelligent Vehicle/Highway Systems (IVHS), is, like the Mesh, is also concerned with the problem of coordinating millions of objects. IVHS enables highways to talk to cars (to warn them about traffic conditions), cars to talk to highways (to predict traffic flows), and cars to talk to each other (letting them travel more closely packed together without fear of collisions). Sensors and software promoted by IVHS may have defense applications, as would associated developments in non fossil-fuel energy.

Health care is an area whose synergies with defense technologies are underexploited. Medical

instrumentation, for instance, is similar to defense systems in their cost, complexity, and the fact that their functionality is a matter of life and death. Cost control requirements may require that more people be monitored outside expensive hospital settings. Doing so would impel the development of remote health sensors that engage in periodic and emergency communication with health networks—a technology with many resemblances to the Mesh.

Reorienting Defense Research: After absorbing what is available from the commercial world, and gathering what might become available from commercial piggybacks, DOD needs to fill the gap with innovations that it develops itself.

At present, the DOD research establishment—with their bewildering mix of technologies, wide variety of paths, and diverse clientele—is largely devoted to countering current capabilities and threats. Too little effort is designed to ward off anticipated threats from emergent technologies. Current parameters emphasize performance maximization (faster, more sensitively, over a wider range of environments), and robustness (versus building redundancy into the system vice components). The latter method produces satellites that cost a billion dollars and carrier battle groups costing ten billion.

To develop the Mesh requires a different direction for DOD's research and development program. The

first requirement is some top-down dicta in favor of information technologies that can be deployed as millions of items in a networked information environment. Such dicta would have to be translated into parameters for systems that can be composed of smaller and cheaper components that can be adapted or derived from commercial products. Second, a developmental bias needs to be inserted in favor of methods that divide system functions into decomposable parts, and develop open interfaces so that it can fit into both today's information mesh and tomorrow's. Third, a bias for bench-scaling, building, and testing should be part of the development process. Fourth, systems planning should anticipate that telematics technology will continue to advance roughly fifty times from one end of the ten-year development cycle to the end. Researchers should look for ways to solve problems in software or silicon-embedded microcode rather than with hardware. Thus one should avoid, for instance, developing precision machinery to align multi-spectral photographs if a computer of sufficient power could correlate the various spectral images and determine what is the most probable correlation between various photographs of the same scene.

Fostering Open Systems

Rapid technological change virtually dictates open systems design. To understand why requires appreciating how much of today's acquisition cycle time is spent integrating component to subsystem and subsystem into a final system. At every level, each of N subsystems have to be fit with each other requiring the simultaneously solution of the n-square problem. Typically, defense systems are very tightly constructed for maximum efficiency. Altering one component changes a subsystem's performance which in turn changes a system's performance and so on. Thus, minimizing unnecessary changes between specification and integration is important. So how are parts to be specified? If parts requirements assume current technology (which most do), parts will be ten years behind the state-of-the-art when fielded. Calling for components with then-current capabilities may be necessary in some cases for mission accomplishment but overdoing it risks the possibility that such performance is not possible or affordable. If so, the program is delayed; conservatively specified components fall further behind the state of the art. Systems that result from the process tend to contain far too much old technology, but at least with stable technologies the benefits of tight integration cover the costs.

When technologies advance rapidly and unpredictably, however, this model breaks down. The

alternative is building systems not from subsystems fit to each other, but to subsystems each fit to a standard interface which is careful specified. This is precisely the approach now being developed for the new generation of object-oriented software modules. As with software, this approach loses efficiency because modules cannot take advantage of known aspects of other modules. However, any lost efficiency is more than made up by greater flexibility. Other modules can get major updates without forcing the whole system to be reintegrated. A new capability, suddenly possible, say, two years prior to fielding, can be inserted with less damage to the original schedule.

Systems integration takes on new meaning for meshes—at that level, it is almost all software. The combination of common components, open systems, and *external* systems integration would redefine defense industry. Today's typical prime contractor, ostensibly a frame manufacturer has, over time, become a systems integrator and software writer. The prime imposes hardware-originated contract specifications upon what are, even now, defense-oriented subcontractors. Tomorrow's prime will be almost entirely a software house. Most subcontractors will have to find markets in the commercial world to achieve the low price, and compatible tools and parts that future systems need.

The rise of the Mesh also informs the current debate over what to do with today's shrinking defense giants. The United States, as well as its allies,

possesses an excellent defense industrial base whose existence and capacity are imperiled by expected defense cuts. Many defense analysts are looking for ways to keep them alive: more R&D, extra maintenance work, or weapons purchases, foreign military sales, or direct preservation.

The usual argument is that such subsidies are wasteful; the more pertinent argument may be that they are counterproductive. Why? The current force was designed to counter opposing and comparably capable Soviet forces almost weapon-for-weapon to engage in like-on-like combat. For the next decade or two, the odds of a new peer competitor are low. The United States has enough good systems in its inventory to avoid needing many major systems starts. Although new systems would be more survivable and perhaps more efficient, neither fact justifies multibillion dollar development programs. Beyond two decades, a peer competitor and thus feature-for-feature competition may re-emerge. But by then, the value-price ratio for information technology may be a thousand times higher than today's and like-on-like platform combat may be obsolete. Many skills (software aside) needed to build ships, tanks, and planes will not be relevant to building meshes. Worse, the persistence of a large platform-oriented industrial base may be inimical to promoting the revolution in operational concepts needed to change defense paradigms. The current defense structure may retard rather than promote defense reconstitution.

Software

Major improvements in software will be necessary to realize the Mesh: remote systems integration (how to get two different systems to recognize and talk to each other), pattern recognition, adaptive algorithms, data-flow architectures, image compression, and simulation. The algorithms required in the Mesh will need to mix deductive digital components (with their formal logic) and inductive analog components (with their dynamic minimization techniques). Software tools per se are inherently dual-use, and many of the algorithms will find use in the commercial world. Some techniques for remote systems integration may be developed for the infrastructure projects mentioned above. At the level of specific software for particular applications, though, the code will almost always be exclusive to defense applications.

Training and testing will become a greater component of software development. Few complex systems work well the first time out; they will miss some targets and identify other objects as false threats. Neural net components, in particular, need to be tuned by repeated example until they are reliable. The Mesh will have to be tested against wily foes; B-teams could generate decoys and false images as well as real targets with unexpected parameters. Meshes will have to learn, as humans do, how much evidence to collect, and which anomalous readings to pitch out.

Wars hitherto fought in real media will increasingly be fought in abstracted media. Although the same banging and shooting will take place, the cue-search-locate-categorize-target-shoot-assess cycle will require not direct analysis of sensory data, but its abstraction in the realm of oughts and noughts. The offense will be as good as the algorithms that power the cycle. The defense will be judged on how well offensive estimates can be frustrated. Many theaters of conventional warfare—space, strategic warfare, and naval warfare—have already been abstracted in that warriors already sit in a simulated environment, one that they no longer directly perceive. This tendency will only become deeper and broader (e.g., pilots will increasingly look at their screens rather than out their windows).

Abstraction implies that what military personnel do—regardless of service—will converge. Successful performance will mix an increasing percentage of generic software skills with a decreasing percentage of media-specific ones. True, the algorithms that train sonobuoys to find submarines differ from those that pick out small satellites from those operating in cluttered jungle or urban environments. Experience with a physical medium yields better algorithms. Yet the underlying skills remain the same: writing maintainable code, using computer-aided software engineering, evolving well considered objects, taking advantage of network resources, conducting fuzzy and discrete logical analysis, tuning neural networks,

recognizing images faster and more accurately, countering deception, improving the efficiency of learning algorithms, integrating systems, wringing more sensitivity from statistical processes—and so on.

The evolution of the aforementioned Information Corps may yield two distinct types of software skills. One group would develop the system, train the Mesh, and maintain the code to new circumstances. The elite force would specialize in restoring a systems *in real-time* against unexpected situations or enemy action. Both forces would work together—original writers often do the best repair—but the grab-bag of tricks necessary to rewrite and retest code quickly may need to be developed especially for military field uses. Such an elite will get considerable use in wartime; the benefits of fooling a Mesh—which is only as affective as its treatment of new threats or new spins on old threats—even for just a day, can be considerable. The elite of the Information Corps would travel globally to install, oversee, reprogram, or trouble-shoot the massive automated systems that tomorrow's armed forces will have become.

Strategic Competition

During the waning days of the Cold War, both manufacturers and controllers of American export worked themselves into a mutual frenzy trying to differentiate weapons from dual-use items that might have a military application. The advent of the Mesh will make this distinction even less meaningful. Because the Mesh requires dense coverage to work, economics requires adopting and adapting commercial items—already made by the millions and billions. The same batteries that power consumer cameras would be candidates to power militarized optical sensors. As world markets continue to broaden, what prevents an enemy from building systems from the same materials the United States does?

Nothing, really, but therein lies a dilemma. Our current military, composed of large expensive systems, is based on hardware that has no commercial substitute, and is largely unmatched by anything in world markets. Even after spending a full day at the world's armaments mall, an adversary starts from a weaker position than ours. To scrap our advantage in favor of a system whose technology base is common to all might seem to aid national security as much as the switch from mainframes to microcomputer clones helped IBM. True, America can still afford more equipment than its adversaries. But even during the Cold War, though, America's military philosophy

always emphasized qualitative over quantitative measures of superiority.

The use of common parts need not translate into common capabilities. The hardware may be the same, but the secret is in the software—as the entire computer industry is learning. True the computer-aided systems engineering tools and many of the fundamental computer algorithms will be the same for both civilian and military applications. But many tasks that the Mesh has to perform—pattern recognition, learning, auto-configuration, counter-deception tactics, and data fusion—need to be reified in specific code. Such code would generally differ sharply from what similar tasks look like in commercial applications. To the extent that the United States would invest tens of billions of dollars a year in building and refining such code, an adversary would have to spend comparable sums to develop a similar system. Capturing a code-intensive device would not be as revealing as for instance, capturing a panel from a B-2 bomber. Microcode embedded in silicon is extremely difficult to reverse engineer; some chips in use in the intelligence community already self-destruct upon opening. Capturing the original source code would compromise security (*if* it is well-documented code). However source code could only be stolen from the factory, not—as with hardware—in the field.

America's wide lead in software is another advantage to concentrating our military functionality

there. This lead is evident everywhere from our dominance of packaged applications to our lead in systems integration for telecommunications and aerospace. Simply put, the American dollar goes further in software than the German mark or the Japanese yen. Thus is multiplied the advantage that our GNP affords our defense. By contrast, American manufacturing skills, dollar-for-dollar are nothing special and, if anything, may be falling farther behind those of our rivals. That said, the ability to manufacture lots of little items—without having to depend on trade partners reluctant to serve U.S. military interests—remains important.

Can the United States still lead in software, or are we facing (*pace*, Yourdon) the "decline of the American programmer"? Without discounting the Japanese threat in software, their inroads into American markets have yet to come materialize. Cities as diverse as Budapest and Bangalore have cadres of over-educated but under-employed programmers who write good code for peanuts. Nevertheless, the best foreigners are more often drawn into our corporate orbits than our orbits are rendered asunder by their companies. The lead is there if we choose to maintain it.

5 *Unconventional Conflict*

The expected triumph of information-based warfare over industrial warfare does not automatically imply its ascendancy over pre-industrial warfare. Nevertheless, better surveillance and communications for both sides will alter the character of such conflict.

If U.S. forces fighting in Korea had had twenty-first century information capabilities, the Korean War would have gone far differently. The original invasion would have been rolled back far faster and the Chinese counterattack would have met far tougher resistance. By and large, the Korean War was conventional. The same capabilities backfit into the Vietnam War, however, would have made far less difference, especially prior to Tet 1968, while the war remained largely unconventional. Information-based warfare works best against industrial-based warfare and much less well against pre-industrial warfare.

Nevertheless, the ability to catch platforms in a Mesh is not entirely unrelated to the ability to catch other things in the Mesh, bearing in mind that similar powers may be put into the hands of insurgent forces as well.

Rural Conflict

Information technologies will have limited but distinct affects on rural irregular warfare. Villages in the South, after all, are likely to be affected last by information technology. In such realms warfare is light on platforms and heavy on cover—physical (e.g., jungle canopies) and virtual (e.g., peasant by day, fighter by night).

If nothing else, both guerrilla and state forces are becoming better connected. Digitally encrypted cellular systems can yield greater reach, much faster responsiveness, and better security for guerilla communications. Reach improves the command and control of dispersed forces. Responsiveness permits flexible synchrony of operations. Security nullifies the value of signal intelligence to state forces. Since state forces tend to have relatively good command-and-control systems today, the relative improvements from information technology will be modest, and their advantage over irregular forces will decline.

Movements of both irregular and state forces would be better tracked through both sides' use of cheap disposable sensors. Here, the change in relative advantage is harder to predict. State forces are already easier to track; they tend to move in larger units on well-known paths. Jungle feet need far more sensors to detect than do road trucks. Thus, until sensors become

absolutely ubiquitous, information technology may, if anything, increase the vulnerability of state forces.

Information technology makes free-fire sensor-mined barriers around "protected enclaves" easier to establish (even though the problem of filtering the good, the bad, and the ugly remains). Using theft from state arsenals to arm guerrillas would also be complicated if weapons were to come with built-in radio emitters. Emitters coupled with arsenal security systems could monitor their own movement and broadcast alarms if theft takes too far from where they should be. Weapons can be recovered faster if they have such devices (until disabled or removed sufficiently far away).

Increased use of overhead surveillance will also allow state forces to track agricultural cycles more closely. Knowing the onset of crop harvests would permit tighter control over resource flows in the rural economy. In nations with scattered and unpredictable harvest times (due to varying crop conditions or topography), for instance, state forces to be dispatched to places where they can have the greatest impact.

Urban Conflict

Over the next several decades, urban conflict is likely to become more important than rural unconventional conflict. Cities in the Third World are not only growing much faster than their rural hinterlands, but in most parts of the world they are growing increasingly independent of them as well.

To illustrate why, consider the world's nations in one of three categories. A billion people live in the demographically stable (if not declining) West: OECD nations plus the former Warsaw Pact nations (less Soviet Central Asia) and the Asian Tigers; Western cities eke out one percent higher growth rates than their countries as a whole. Another billion plus live in China, whose population growth is decelerating but whose urban growth is accelerating to near four percent. The rest live in the "South"—the Third World—whose population growth, at two percent, is rapid, and whose cities grow two to three percent a year faster. The following table compares 1990 and 2010 total and urban populations of over one million souls. Bear in mind that everyone who will be sixteen or older in 2010 has already been conceived.

Population by Region and City Size: 1990, 2010
(in billions)

	1990		2010	
	Total	Big Cities	Total	Big Cities
West	1.2	.4	1.2	.5
China	1.1	.1	1.3	.4
Other South	3.0	.4	4.5	1.5
TOTAL	5.3	.9	7.0	2.4

By 2010, one of every three will live in cities of greater than a million; these cities will account for over half of the national income in all three groups. *Total* city folk (including those in smaller cities) will exceed total rural folk.

Cities of the South will also evolve in another respect. A tenet of Chinese guerilla warfare presumed that such cities lived off the country, making agriculture the only true source of wealth. Cities only served countryside, created markets for their goods, provided low-technology manufactures (often imposed on rural consumers through trade restraints), and housed their masters (and those who served them). Third-World nations entered global trade largely by

selling commodities originating from farm, forest, mine, and oil patch. Thus with the countryside taken, cities—deprived of their livelihood—would fall.

Southern cities are now becoming export centers in their own right and depend less on their hinterlands. One reason why is demographics. The larger the percentage of city dwellers in a country, the harder it is for them to live off the countryside. Extracting greater surplus value through taxation, price controls on foodstuffs, command transfers, or import restrictions just retards the entire economy. Conversely, the same factors that boost world trade (cheaper transportation and communications) create export opportunities for low-wage urban manufacturing (as well as contract services, and tourism). As Western economies open to Southern manufactured exports, Southern cities are opening to Western investment capital.

Prototypical Third-World cities are becoming weaned from their hinterlands and are participating more in the world's trade network of things (ports), people (air traffic), and information (telecommunications). Physical and virtual networks are complementary. Although talk can replace travel, the more people talk the more they want to meet. Cheap travel lets bright Third-World students go to American universities and return; the experience makes them want to stay plugged into America's Net. Networks linking cities of the South to those of the West will lag those which connect the West's cities (and their

hinterlands). Yet fiber optics, cellular and satellite networks, combined with data manipulation and compression techniques make the former better all the time. Trans-Pacific air travel keeps growing at 10 percent a year; trans-Pacific telecommunications, perhaps twice as fast. Miami is, if anything, strengthening its status as the capital of Latin America.

Because cities are better networked than hinterlands, the growth of Southern cities, in and of itself, puts a larger share of Southern populations onto networks. Moreover, capacity in the Net is getting cheaper to build. With the increasing participation of third world cities, the world is increasingly becoming a network of networks.

When Southern cities were a smaller fraction of the national total, basic insurgent strategy was to exploit village resentment of urban elites to first win over and next control rural populations (taking advantage of their relative isolation). The occupation of enough rural territory left cities ripe for takeover. Urban growth and autonomy hits this strategy on two counts: the strategic mass of the countryside is relatively smaller, and rural cut-offs have less impact. To conquer a country requires taking a city on its own terms.

As with rural conflict, information technology can help (and thus hurt) both sides in urban conflict. The methods of urban unconventional conflict—on both

sides—mirror those of crime fighting, notably gang warfare. Organized political assassination is not too different from random assassination here. Terrorist acts resemble vandalism and arson. Many urban guerrillas are financed, in part, through crime against property. Street gangs fill their arsenals by robbing gun shops; guerrilla factions could do the same.

Such analogies have their limits. Although urban gangs vie for control over certain facets of urban life (e.g., protection)—and thus challenge the state—they rarely seek to displace all state power. Gangs have little interest in certain acts—seizing radio stations, calling out street mobs, creating an alternative legitimacy—otherwise undertaken by insurrectionists. Where law has broken down entirely and many urban services have ceased to function as in Beirut, urban warfare more resembles rural conflict. Active control over neighborhoods under such circumstances is analogous to active control over village districts and is as hard to pull off.

How states combat urban terrorism depend on the values of the body politic. Certain techniques that technology permits may nevertheless be forbidden by a sincere belief that certain methods are entirely too intrusive. Totalitarian societies are rarely bothered by such scruples, but, as Eastern Europe's recent history suggests, a lack of scruples does not guarantee the long-term security of the state. Over time, if an organized threat—if identified as such rather than

ascribed to general urban chaos—starts to pinch, the body politic may tilt toward harsher security practices. Conversely, in states opposed by a sufficiently vocal urban sub-class, arguments for civil liberties may mask a more fundamental desire to overthrow the state.

The greatest help in identifying both criminals and insurgents is a body populace sufficiently outraged and uncowed to turn opponents of the state into the police. Failing that, information technologies can do only so much, but what they can do is worth noting. By 1995, systems in the United States will let police identify anyone from fingerprint records within a minute. GPS transponders in police cars are capable already of recording their position in real-time. DNA fingerprinting is becoming more reliable, and ever more minute samples can link perpetrators to crimes. Voiceprinting can also be used as a form of identification. Both will become more efficient as larger data-banks become available. Similarly, key documents such as drivers' licenses and passports can be made forgery-proof (today's methods use holographic imprinting). In addition, large, easily accessible card-to-face data banks could make it extremely difficult for one person to hold two cards.

Although sufficient computer power to link identifying information, certificate information, financial records, and telephone records exists today, the American consensus holds that such linking would sharply reduce individual privacy. Even those who

trust the government understand that such data repositories can be broken and entered by individuals and corporations with even fewer scruples. The value of such correlations in fighting crime and insurrection is limited. Law-abiding citizens are much more likely than criminals—who, for instance, pay cash—to leave large data files in their wake. However, other countries are less concerned about either civil liberties or such distinctions than we are.

Certain computer technologies may afford the state greater control over those captured by state forces. Virtual reality technologies, for instance, could make interrogation and brainwashing, if not more efficient, then at least less costly (since human attendants need not be present for such sessions).

Sensors can also be used more intrusively in the urban environment even though such moves may be resisted. Many toll booths take snapshots of license plates driven by toll evaders. A system that could read (rather than take a snapshot of) the tags automatically could be easy to add. Putting such systems on heavily used streets coupled with computers powerful enough to correlate license plate (and car make) permit organized tracking of people's vehicles. Similar overhead surveillance can be used on battlefields and in urban settings. Image recognition software that could identify faces inside cars or on street corners will come, albeit in a few decades.

Other sensors of use would be aural sensors for picking up stray gunshots or explosions. Sensitive ones might also recognize voices. Olfactory and other chemical sensors could also pick up traces of violent crime as it occurs (e.g., gunpowder). If sufficiently sensitive they could determine identities much as well trained dogs can. Seismic and acoustic sensors could determine the weight of a passing vehicle. Lasers reflected against windows can hear conversations inside. Again, the deployment of such devices in various cultures will vary according to national mores. Such mores differ. Supposedly, while Americans during the Cold War were particularly incensed at the Soviet eavesdropping; Soviets, in turn, were outraged by our overhead surveillance.

Yet all is not lost for those who would conspire. Its literal manifestation—to breathe together—may be anachronistic when video teleconferencing can replace face-to-face conspiracy. As earlier noted, such conferences can be digitally encrypted to a fare-thee-well. Telephone tapping may, under such circumstances, become a lost art. Sufficiently motivated conspirators can even avoid records of their having talking to each other by using a private switch that does not log ultimate call destination. Computer technology facilitates establishing highly compartmentalized cells in which no one knows the entire organization. Indeed no one need know anyone else unless face-to-face contact is essential. Using E-mail removes most identifying features of the

respondent compared to voice. Even if police informants could enter a conspiracy and learn implicating data, the degree of infiltration can be far better limited than in the past.

The disadvantages of stealth, of course, are irrelevant for conflicts that go public. The political use of crowd psychology still requires a physical crowd. As more political discourse takes place via two-way television and E-mail technologies, gathering people for political purposes becomes that much harder.

Another relic of previous urban conspiracies may be the old trick of storming the local radio or television station. Not only does storming the core node of a cable system (often separate from the multiple contributing broadcasting studios) lack the panache of storming a radio or television station, but it may be ultimately irrelevant. The proliferation of multi-node cable, direct broadcast satellites, redundant cellular systems, and video-on-demand through the phone system will put to rest to any notion of a centrally controlled source of information. Such infrastructure makes it is difficult to shut up a government, its rivals, or any splinter group. One of 500 channels out there will always feature someone.

Net States?

The information revolution, acting through multinational corporations and transnational communities, may weaken many powers of the state anyway. Would it be much of an exaggeration to posit a nation's expression, not through government, but as a local ganglion of the world Net. That being the case, might not the decline of the state coincide with the rise of the Net, the newest venue for crime, conflict, and chaos?

6 *The Net and Its Discontents*

The Net is the converging global system which puts people and their information in close electronic contact with each other. The growth of the Net, by permitting subnational and transnational communities alters the basis for international conflict. The Net, itself, however, presents certain exploitable vulnerabilities for societies that depend on it.

Patterns of war reflect the relationships of individuals, the communities they form, and the nations they live in. The information revolution has already and will continue to alter this flux, but in unexpected ways. Thirty years ago, the glib consensus was that information technologies would create a global village; to a large extent it has. The further rise of the Net—a future complex of sensors, processors, and communicators—will create global villagers. The new villages will be unbound by geography, but bound by their own parochial reflexes. They may find new and exciting ways of getting along.

The impact of the information revolution on the sources of conflict—the political construction of societies and the expectations of their members—is both more and less obvious than its impact on purely military operations. Most of the technology necessary

to power the civilian side information revolution has already been invented; it only needs lower cost (as happens continually) and wider distribution. With it comes the elaboration of the information revolution to new uses and new users (particularly in the South). Harder to assess is the dynamic of commercial competition in information markets. Military revolutions tend to be driven by well-known forces. Technologies proven useful are likely to be adopted by someone. Once they are demonstrated, complementary and countervailing capabilities follow. Commercial competition is a complex game involving competing vendors and multiple consumers with varying needs. Only some of the possible converts to the probable because the calculus of individual desire does not lead to a closed set of outcomes.

In its commercial adaptation, the Net is, in one form or another, inevitable. The declining cost of acquiring, processing, and transmitting bytes will call forth an infrastructure which puts people (and their machines) in closer, faster, and denser contact with each other. The Net may be likened to our phone system extended first globally, and then to every possible digital device, removed from its land-bound linkages, given the power to transmit multiple video streams, and overlaid with enough filters and translators to find every needle in the global haystack.

The impact of information technology can be discussed in terms of five broad trends: the erasure of

distance, fixed and floating networks, universal translatability, the mutability of truth, and, as a consequence of all this, the rise of the global villager. This forms the context of national security. The next section deals with the ghosts in the Net.

From Global Village

By and large, the information revolution has spread knowledge faster than fearful governments can slow it down. Cheap cassette players and tapes help spread the 1979 Iranian revolution. Fax machines helped power the 1989 uprisings in Tiananmen Square. Leaders of the Soviet Union's abortive coup in 1991 failed to appreciate how modern telecommunications (e.g., voice, video, and E-mail) in the hands of those who understood them (e.g., allies of Boris Yeltsin) could become such powerful weapons. Although ham radio operators in Bosnia did not stop atrocities, they have prevented their taking place in secret. AsiaSat is sending television signals that travel past the reach of censors. Traditional regimes cannot easily control the information that their populace receives. However, if a populace like the Serbian does not wish to hear bad news about itself, only modest amounts of media repression will be sufficient to keep society closed.

The ubiquity of broadcast media has CNN-ized perception—hence, world politics. The instant access to world news available in the United States since

roughly Huntley-Brinkley days is now available overseas as well. Many world leaders talk to each other via CNN and other networks. This capability has forced the West to respond to suffering in places such as Somalia otherwise beyond public attention.

Yet, cheaper telecommunications, while obliterating the dominant role of propinquity in creating communities, cuts both ways. It is easier to create communities that traverse geographical boundaries, but it is harder to find a unifying force or a common set of cultural assumptions in communities that are defined only by geographical boundaries. The state is not ready to wither away, but its suzerainty over a world of global villagers (despite some resurgences of nationalism in the second world) will be redefined. Such redefinition could affect national security much more than would the advent of battlefield meshes. The latter come into play only during those rare moments when strife erupts into war.

The Erasure of Distance: The cost of doing business over wide distances (especially overseas) will keep dropping dramatically. The volume of international calls will keep rising briskly, and low-power cellular phones are likely to, in ten years, permit satellite-connected phone calls from anywhere. Most cities will also have the infrastructure for dial-up videotelephony. Emerging technologies of virtual reality could let people sense, in whatever detail required, a physical phenomenon (e.g., a

malfunctioning refinery, a wounded person) half the world away.

The reduced cost of coordinating a world-wide enterprise will strengthen the internationalization of corporate business, particularly manufacturing. Whether or not corporations then become truly global, the competition between semi-skilled workers in the West and skilled workers in the South will grow sharper. Joining footloose manufacturing will be footloose backroom services and perhaps even some frontroom services that require face-to-face contact.

This transfer cuts both ways. On the one hand, check processing, for instance, is moving from South Dakota (itself relocated from Manhattan) to Barbados. On the other, thanks to remote virtual sensing that allows a person here to manipulate robotic instruments there, a surgeon in Chicago, could work on a patient in Caracas who would (if awake) perceive the doctor as an apparatus.

Freer communications tend to cut the cost of conducting both routine and knowledge-intensive business in the South. This should work in favor of broadening economic growth (competing with other factors that will narrow it). The easy spread of text and image could spread education everywhere and thus most help bring Southern workers to Western standards.

Other barriers to business that derive from differences in language or currency would also fall. Computers that can recognize anyone's speech will reach the market by the mid-1990s (replacing systems that must be trained to the nuances of each speaker). Language translation is making comparable progress. Good but slow and domain-specific real-time translation is already possible. Newly invented devices can read signs in foreign languages and flash the translations to video devices such as "heads-up" displays associated with your glasses.

In the meantime, more people will want to learn English to understand the growing warehouse of entertainment and educational material about to become globally accessible on-line (just as they now learn English to conduct business). Most people who have attended high school anywhere in the world should know English well enough to talk without translators.

Similar barriers are falling in currency translation. Electronic banking and the virtues of automatic currency markets will let people keep bank accounts with equal facility in any currency (unless governments stand in the way). Money, after all, is a measuring rod of value just as a yardstick indicates length. Exchanges and contractors can be denominated in them even if neither side owns them. Thus, little prevents considerably more business in the South from being conducted in Western currencies. This is good news

for countries plagued by high inflation and unstable currencies.

Globalization, in the 1980s at least, promoted old fashioned liberal values (e.g., free commerce) in both West and South because if freed wealth from state influence. The information revolution can only deepen such trends. When wealth is reified in physical, largely immovable objects like land, resources, factories, and buildings, it is subject to diversion by governments. When markets must be serviced from local sites, the state gains similar leverage. As more wealth is contained in the movable intangibles of information, or when markets can be served from anywhere the influence of the state recedes. Ultimately, major corporations can be run out of a collection of networked briefcases each situated in one or another vacation spot, where the weather is equable and the taxes are low. In the 1970s the South imagined the golden road to wealth led from control over resources; hence governments tried to raise the prices of commodities they commanded. In the 1980s, the surer road was to create a subservient but well-educated workforce that multinational corporations could exploit or trade networks could tap. In the 1990s and beyond, savvy nations will complement human capital with dense robust information infrastructures to jack their growth path upwards.

The Global Net: Traditionally, the South (and rural West) was characterized by a sense that its

denizens were simply out of touch with the greater universe. The ubiquity of the Net will connect individuals and give them access to a vast library of knowledge. Its core will, more likely than not, be the global Internet and its fifteen million subscribers (and growing fast). The Internet provides a vast, fast, and reliable electronic mail network, the ability to download information from public files located anywhere, and support for on-line news and bulletin board groups of every shade, variety, and flavor. All three foster the growth of global communities linked by interest and earlier separated by geography.

With time, the Net should allow anyone with a video-input-phone to see the world's accumulation of organized information: scientific and medical articles, papers, books, serious journals, newspapers, photographs, and maps. Navigating through such seas will, at first be daunting, but tomorrow's information pilot fish, so-called "know-bots," would stand by to swim through this enormous data base. With growing sophistication, it could find answers for those questions that data can answer. Personal filters could cull listener-specific news items from the glut of world news broadcasts and other sources of new information. Global access to the Net facilitates education and business from all ends of the globe. Moreover, it overlays the economic potentials of the West atop Southern societies which are structured to cope with far more restricted economic and social potentials.

The communications revolution will also accelerate the transfer of open-source defense-relevant technology, making it much harder to control. Any computer chip reducible to an algorithmic formula could, one day, be manufactured in one of hundreds of facilities. The world will not lack small rogue fabrication shops willing to evade export controls to make money. Technology control regimes for unclassified software and micro-electronics will be virtually impossible to police.

Inevitably, every device worth talking to or hearing from will come equipped with low-power communications, high-power computations, and a virtual address. Networks will increasingly link equipments—automobiles and other vehicles, traffic lights and toll booths, factory machinery, remote cameras, various utility meters, medical and scientific instrumentation, and instruments otherwise useless if not network—rather than people. Mobile equipment with GPS receivers will communicate their location periodically. Coupled to this network will be various sensors used to monitor certain environmental activities such as weather, soil conditions, toxic emissions. Others would monitor the health of the sensitive measuring blood chemistry, brain wave readings, heartbeat, perspiration, pneumatic functioning and so on.

What will they all talk about? Remote operation and monitoring of machinery may be a major topic.

Cars and traffic lights will have long and loving conversations about road conditions. Devices will babble, "I'm OK, are you OK?". Note this picture of the future city—all these networked sensors coupled with intelligent nodes—increasingly resembles the Mesh (without rockets). How much technology separates the sensor-rich automobile increasingly sensitive to its immediate surroundings from a sensor-rich tank?

On the one hand, building the Net requires all these devices interoperate so that their communications protocols, data formats, and associated algorithms work with each other. The amount of attention paid to standards will undoubtedly rise even though increasing computer power would make the operation of gateways, translators, and virtual device layers less visible to users.

Ironically, the groups that represent the various connected domains may even discourage communications that standards supposedly permit. Should that seem odd? Communities ranging from the professions to street gangs maintain their own jargon. Ostensibly they (or least the professionals) cling to a separate jargon to make precise distinctions unavailable from ordinary language. Yet the more powerful motivation may be unstated: to exclude outsiders (for whom a little knowledge is dangerous), establish status distinctions, or preserve privacy. The Net that unites also divides.

To Global Villager

What turns the world into a global village, with everyone capable of looking over each others' shoulders, may also promote the creation of global villages—communities of interest and inclination that span the globe but let members isolate themselves from others outside.

CNN, for instance, not only lets you keep tabs on the rest of the world, but also lets you keep track of events at home when you are on the road. Thus can a community of expatriates (e.g., Iranians who live in Southern California), better maintain their isolation from the worlds outside their door and remain united in a common lingua franca of interest. The Net's ability to connect people with the world is what allows them to identify their own communities, archives, and news groups and pretty much stick to them.

The Chinese expression "same bed, different dreams" carries over with fuller force to the evolution of perception. By mid-Century, for instance, the reduced costs of transportation and communications forged a mass American consumer market from a collection of smaller regional ones. Further declines in the cost of communications and computer-driven direct mail promoted subnets which further fractionated it along various demographic, professional, avocational, religious and ethnic lines. Communications at first

enables the CNN-ization of perception. Continued evolution results in de-CNN-ized perception and the rise of the same voluntarily isolated communities that pre-date mass consciousness. This time, though, such communities will subset and superset national boundaries and thus the states that govern them. This distinction could matter a great deal to how national security is defined and ensured.

Cellular technologies exacerbate this trend. Text-oriented desk-bound computers are weak devices to maintain communities. Few want to live tethered to a box and bits alone cannot convey the look, sound, and feel that normal human contact requires. With cellular, the network need not be associated with a fixed phone connection and box. Voice commands make keyboards unnecessary. Screens can be built into eyeglasses. The basic box can be shrunk to the size of a hearing aid. You need never be out of effortless touch with your virtual community or it with you. Virtual reality may be so compelling that people need leave only to eat and exercise (perhaps the resemblance of this description to a jail cell carriers deeper meanings).

Thus, although information technology can bring the world together and erase bonds of geography, they also let utterly different communities maintain their identity against assimilation.

The Mutability of Truth: As the amount of information increases, its marginal utility declines, but so does its veracity. Why?

Start with broadcasting. Today's satellite broadcasting systems relay material to terrestrial broadcasting stations which then relay them to television sets. Tomorrow's systems will reach television sets (equipped with 18-inch satellite receivers) directly—bypassing the investment in both television stations, and the political control that nations can have over transmissions.

Virtually every Third-World village is likely to have at least one such television (even if not on the national electric network) and probably several. Each can watch hundreds of stations, only a few of which will be state run. Video signals from space will be harder to jam. Barring state confiscation or control of such sets, they should be able to get a video signal from any group with enough money to rent satellite space. Just before Desert Storm, President Bush asked for permission to appear on Iraqi television to explain our actions in the Gulf. Two decades hence, his successor will not have to ask. Dictators will be hard pressed to keep rivals off the air. No coup plotter could keep his prey off the air either. By the same methods, conservative regimes will have difficulty preventing the diffusion of the West's best values over the tube: sex and drugs, rock and roll, and guns.

Technology will also make it impossible to distinguish among real and fake photographs, video, or recordings. Anyone with a good machine (tomorrow's Silicon Graphics box, perhaps) could create for broadcast a video of an opponent counseling acquiescence to his people. This image would look and sound like the real thing, being indistinguishable in both grammar, nuance, and gesture. Western audiences, more used to special effects manipulation will grow skeptical of everything on the tube after a while. Third-World audiences are likely to remain credulous targets a good while longer.

These two trends—the ability to force information past controls, and the ability to create false information—work both with and against each other. People tend to believe what they want to believe (or what others they fear or respect want them to believe). Contrary reports can be easily discounted, particularly as people come to understand how easy faking a video can be. The same technologies that let people freely experience the world are those that allow people to deny its reality. The resulting cynicism works in favor of people trusting only the information generated by their own village—not the globe as a whole. Reality is not universally validated but personally validated based on networks of trust.

At the same time, the privacy and authenticity of personal communication is likely to improve. Current mobile phone communications are even easier to

intercept than line-based communications are; cellular is generally considered unacceptable for secure communications. Thanks to the digital telephony, public-key cryptography, and free silicon, secure digital communications will need but one cheap phone chip. Encryption will be so easy as to be norm. Such encrypted messages will be unbreakable by any supercomputer. Eavesdropping would have to take place at the source or the destination but not in between. Intercepting signals intelligence as a way of figuring out the what the other guy is doing will soon be useless.

The development of digital signature technology will also lend authenticity to private communications as well. Digital signatures work by having people post public keys which alone can unscramble messages. Successful unscrambling proves that only the person with the corresponding private key could have written it. Such techniques also keep third parties from altering the message without its being obvious. All this assumes that the posted public key is authentic and actually linked to the poster. Such facts may have to be verified, again, though a trusted network—again, the global villager at work.

Today's virtual reality is far more virtual than real. Tomorrow's, though, may look, sound, smell, and even taste, and feel as real as reality. Information technology alone will not convince the sane that the virtual reality is reality (prosthetic reception devices are

one reason why); yet it can convince them that virtual reality is better.

The New Parochialism: Would all this communication among groups hitherto separated by language and geography make people more or less likely to deal with each other in friendly and civilized ways?

Ubiquitous communications could promote a global superclass transcending national boundaries. If this class can define a sufficiently tight set of class interests—an issue of more-than-academic consideration every since Marx—transnational warfare may be muted (but perhaps at the expense of class warfare) in some ways. Other less exalted supra-national communities—linked by bonds of profession, ethnicity, or avocation—are possible. Whereas such communities have always existed, technology will let them conduct a much larger share of their daily interactions with each other.

Would the formation of supra-national classes make their members feel more solidarity with each other and less with their local community? Would they be more likely to respond to attacks on outposts of their superclass, or would all this communication only remind people how deeply different national origins impress their marks on otherwise similar people? Will inter-ethnic communications lead to greater understanding and thus more tolerance? Conversely,

would a little knowledge delude people into thinking that they understand how others think? Internecine conflict is often far less civilized than similar conflict among those who originate from opposite ends of the globe.

The ascendence of Net over Nation could alter what people would fight over. Historically, wars have involved challenges to territorial control—and not just because everyone has to live and work somewhere. Before the industrial revolution, rural land was the source of wealth. The industrial revolution made factories, infrastructure, and resources—all of which could be physically seized—the source of wealth. Even today's post-industrial service economies are tied to place. Otherwise why would so many put up with Manhattan when Maine or the Ozarks would be much more pleasant? Yet, the true assets of Wall Street—the knowledge, connections, and legally valid financial claims—are, themselves, place-independent.

As networks expand to enable better remote communications, the validity of holding on to any one place becomes increasingly questionable. A future Hong Kong could as easily be relocated to Vancouver or even to a hundred Chinatowns scattered about but networked together. Singapore has a core competency in bulk materials handling not only because of its port, but for other reasons such as knowing how to conduct intermodal transportation efficiently. Such knowledge could be transferred to any other similarly wired port.

Today's multinational heavily networked knowledge-intensive corporation is an increasingly movable feast. That being so, push less often comes to shove, and more often to slide. Data does not even have to be sent ahead at the last moment; it is already distributed to begin with. People need but change their real network addresses; their virtual addresses (the ones people write to) stay the same. The less wealth can be captured by physical possession, the less motivated others will be to use physical means to capture wealth.

The shift to Net from Nation lets communities be knit by constant communications regardless of place. Communities without political self-governance can maintain their cultural mores by establishing their own subnetworks as self-contained universes. Eastern Europe is seeing its fiercest fights over ethnic and linguistic cultural clans used to contesting over limited media space. A single medium suggests a single culture broadcasting its own values in its own language to everyone else—to wrest oneself free is to band together to form a competing state. Multiple media, however, suggest the support of multiple cultures. As information technology spreads, any group can turn inward in a broader variety of ways—fostering its networks apart from state or majority interests. True, a believer can be reinforced in his fanaticism by picking and choosing among competing media so that no contrary view intervenes. Such choice could exacerbate the energy of those who sought to impose their culture over others. Yet the ability to carve out

separate media spaces also lessens the angst of those who wish only to keep their culture from being trampled upon. It will become increasingly easier to tune out the rest of the world, for better or worse. The expansion of communications (and easy syntactic if not semantic translation) and ability to accommodate separate domains gives competing cultures room to roam without collision. Hence, more *sprechenraum,* thus less strife.

Otherwise, traditional cultural mores will be harder to maintain in a high bandwidth society. Traditional cultures maintain themselves through the coercion of geography (village life is all they know), custom, and language. Failing that, maintaining group cohesion by coercing less affiliated members (e.g., the restless young and worldly intelligentsia) leaves community-imposed censorship. All these are harder to maintain when anyone can get access to any information. Thus, as Iran's experience presaged, traditional cultures in an urban environment have to become more aggressive about such coercion. Minority subcultures, kept to themselves, posed little threat to the transmission of traditional ways. In the Net, they can create temptations for young of the majority communities. Hence more strife, even though traditional cultures are fighting a losing battle, regardless of how vociferously waged in the coming decades.

The ability of information technology to promote trans-national communities does not mean that every or

even most people will become avid members of them. In the West, most people are part of several communities simultaneously: professional, avocational, ethnic, neighborhood (or some are members of no community). Even where they arise, dispersed network communities are unlikely to be so tight as those which live together (cults, for example) and rarely so large as to threaten the state to any serious extent.

Ghosts in the Net

The dependence of cities on networks, both internal and external, creates—as all dependence does—a major vulnerability. This vulnerability is likely to take different expression in the West and the South. For the foreseeable future the Net will be more important to Western economies because the West will realize a higher percentage of its value added from Net flows then the South will. Thus, its vulnerability will be greater, and the payoffs from the Net's subversion to private ends will be greater as well.

Yet, network warfare is likely to be most salient in the South, and politicized from the start. Binding Southern cities into the world economic network draws them into a game whose rules are written by the West. The more important the Net is to a city's life, the more a city depends on an external order of things and the more independent assets are from the state apparatus (and thus also from social claims). Networks are also

avenues of cultural infiltration. The ease by which information can pass back and forth challenges the social controls exercised by closed systems (a problem that even efficient states such as Singapore will have to contend with soon).

Societies that depend on the Net can be attacked by harming the Net just as industrial societies can be attacked by shutting down electricity. Losing faith in the Net is akin to losing faith in the State. Overt threats against the Net may yield useful concessions. Picking up the right information on the Net can be used to pressure individuals. Subverting the Net may yield illicitly gained resources.

The Net may also be targeted for no other purpose than to return society to pre-Net days. If differential access the Net has too much influence over the distribution of a wealth, losers may wish to change the rules of the game, or failing that, end it. Those who do well may nonetheless resent the power of a non-human system, particularly one, which, unlike the phone system, makes judgements on people's needs. The very notion of a Net that can permit any idea to be exchanged is antithetical to cultures that prefer hierarchical control over ideas.

Networks are thus vulnerable, and totems themselves for attack by forces of the extreme left and right. Future unconventional warfare will target such vulnerability; insofar as the United States supports

legitimate regimes, it must find ways of countering this threat. Conflict in the Net would be represented by systematic and organized attempts either to corrupt the operations of the Net or subvert them. The former would strike at the growing heart of tomorrow's urban economy; if people cannot trust commerce over the Net, they would, with no small dislocation, have to revert to earlier systems of commerce whose paths would have become rusty with disuse. To the extent that governance depended on the Net, attacks on the Net, would strike at the legitimacy and effective control of the state.

Attacks on the Net can be categorized at three levels: physical, syntactic, and semantic—ranked in descending order of risk as casually observed. In practice, the reverse may be true.

Physical attacks on the electronics and wires of the Net (switches, trunk wires, major databases and other key nodes) is certainly possible, but, in and of itself, not a new kind of warfare. Industrial-era targets of the electricity, water, natural gas, transportation, or broadcasting systems will remain equally juicy targets. Moreover, most targets of the Net are both harder to find (because they lack distinguishing physical characteristics), easier to protect (because they tend to be relatively small compared to other key targets), and cheaper to make redundant (particularly the few nodes that hold really critical data). Physical attacks will nonetheless ensue, but society's vulnerability to them

can be substantially lessened by appropriate and not expensive measures.

The possibility of *syntactic* attack—one which disables the operating logic of the Net and cause it to crash—is considered very scary. The wars between security forces and hackers will be relatively continuous and they will escalate on both sides (security systems will get better, but new opportunities for mischief will arise, and hackers will get wilier). By and large, however, such attacks will be of minor consequence.

To understand why, start with the celebrated computer virus. Infecting a stand-alone PC requires the user attempt to run an infected program (or what is very similar, try to start with an infected diskette) most of which are bootleg copies of something which, in legitimate form, is mostly safe. Merely uploading a piece of bad data is relatively harmless (for the time being). A computer over the net is a potentially larger worry (because the carelessness of one can infect many), but network operating systems are generally better protected than the operating systems of individual PCs. Indeed, every successive generation of operating systems has security systems increasingly immune to attacks from both remote (e.g., a passed-along virus) or connected attackers. Because most viruses require the complicity of the victim to function, they are unsuitable for anything other than random terrorism. Networks with conscientious users and well-

engineered security systems that do not pull programs from the outside are relatively safe. Isolated computer systems are even safer. Thus, the notion of broadcasting viruses to weapons systems, for instance, is specious.

What limits today's viruses is the fact that, although systems accept data from random external sources, they rarely accept programs and only the latter are the venue for viruses. Programs act (and can thus mutate), but data is only acted upon. No data in a well buffered computer can cause the latter to crash either.

Tomorrow's networks will be different, and more vulnerable thanks to four interrelated shifts in how computers are used. *Remote procedure calls* and *object-oriented programming* mean that the hitherto safe practice of passing data around will be replaced by the not-so-safe practice of passing data-specific programs around with the data themselves (ironically, object-oriented practices were designed to make computing safer). As office networks expand to campus, corporate and finally to global networks, *global direct addressing* will allow every byte on anyone's computer to be addressed directly. Tomorrow's 64-bit chips can point to a thousand times more bytes than the world's existing stock of computer-archived data. Finally, tomorrow's networks are likely contain *floating filters* that roam the silicon prairie looking for game. Know-bots, mentioned above, will be launched by those seeking the ephemeral needle in the

infosphere haystack. Auto-filters, in turn, sift through information that others are sending you, inserting some into active programs, bringing others to a user's attention in priority order, and trashing the rest.

In short, tomorrow's active networks are likely to be shuttling, not just data, but code back and forth. The success of syntactic attack—that on the core operating functions of a computer or a network—depends on what protections are wired into tomorrow's computers. Tomorrow's computers are likely to be better protected than today's microcomputers (where virtually anything can be altered by an operating program), but networks might allow errant code to travel through the network until it finds an open door, buries itself in code too complex to manually find and waits for an external event to awaken. Here, hackers may actually do some good. Uncoordinated hacker attacks that reveal system deficiencies will be responded to with security fixes that leave basic operations intact. Another and greater piece of cleverness would then be required to conduct a follow-up attack. Coordinated attacks which leave many errant programs lying latent may do considerably more damage.

In general, the more critical a system, the more protected its architecture will be from successful attack. Military command-and-control systems are likely, for instance, to be built around nodes that do not accept code except from trusted sites. Money transferring

institutions are also likely to have tough security systems. Digital signatures will be required to transfer money (and only a few people will be able to move really large amounts). It would be foolish to predict that such systems cannot be subverted, but most such subversions will be inside jobs, and, as such, one-shot deals.

However, these four elements can be also be recombined in new and wonderful ways that increase the risk of *semantic* attack. Tomorrow's networks are likely to see the silicon equivalent of conversations between intelligent agents. Consider remote medical diagnosis between a sensor suite that monitors your health and a collection of doctor modules. The latter assess the data, consult with each other, perhaps awaken a specialist, and, in concert, negotiate a series of actions consistent with your values, life-style, and means. The task of obtaining a loan might otherwise require sifting through a thousand banks each with its own rates, restrictions and criteria. Most people would pick a handful based on sketchy or irrelevant criteria (familiarity, propinquity) and start to negotiate with them. The Net permits launching a thousand requests into the system—each of which is trained to understand your requirements. Each request, in turn, interacts with a similar software from a bank, with, in turn, its sophisticated set of questions and conditions. These conversations result in one or a few choices, which may be dispatched with the usual character assessment

via eye contact, but most of the work will have taken place beforehand.

Note, here, how many soft points can be found in the system. A thousand banks now have access to at least some information about both you and your plans. You, in turn, have information on at least some of the lending criteria of a thousand banks. The Net would feature traveling images of our wants, needs, and resources running around interacting with compatible images of the wants, needs, and resources of others.

The challenge of semantic subversion is that false statements will be inserted into the network as real ones. Systems will be vulnerable until well after the mismatches between various inputs and sensors becomes obvious. Such attacks will affect even those chunks of military or financial systems that collect, analyze, and distribute information: those that which negotiate the transfer of information, create profitable patterns of artificial intelligence, and make assessments about the outside world, where the greatest danger for subversion is possible.

Errant code can attempt fraud at levels that a human would find untenable. Consider the bank loan example. Code can survey more banks in less time than a human. Unless a bank's program has random elements, its logic can be figured out by hitting it with a thousand different cases and looking for patterns, biases, and even flaws. Code can keep a poker face

and is undeterred by punishment; thus it can be a much more efficient and determined prober than humans are. Once criminal computer code can be reliably connected to persons, the cost of subversion rises—thus anonymity is key. Security may, in turn, come to demand a digital signature before a know-bot is accepted into a system. A master list of digital signatures would be correlated with some physical manifestation of a user (e.g., a snapshot, fingerprint or DNA print). The tolerance of Western societies for what is essential a national identification card, however, is untested. Systems that hold signature password owners accountable for damage done in their name must account for users whose passwords are compromised (especially if holding a signature password may not be an entirely voluntary act in a wired society).

Humans have a high bandwidth for input and a low one for analysis; computers are the opposite, they cannot forage for data. If launching event probes into the Net teaches attackers how systems react, they can prepare false events that trigger a false system-wide reaction. For instance, if a nuclear reactor turns itself off should it detect several precursors to an earthquake, false precursors could be fed into various sensors and from affiliated computers to effect a power crisis. However, precisely because such events are predictable and fixed, they can be tested for and requisite sensors can be programmed to weed out such false inputs.

Another source of vulnerability might be created as computers learn how to learn. Today, how computers handle the same data varies little from day to day. Tomorrow's computers, however, are likely to change with experience and adjust to the human vicissitudes of taste, fashion, and circumstance (after all, they exist to serve us). Yet, such adaptability makes them vulnerable to false learning based on a flood of false data.

Return to the medical example. Perhaps incoming case data on a new drug indicates a higher cure rate for its target disease with fewer side effects—hitherto, say, increased susceptibility to caffeine addiction. The word goes out to prescribe the drug more frequently even though the new cases are false and the new version is very similar to the old one. The result is far more caffeine addiction in the real population, and a sharp loss in the credibility of the medical network.

Return to the bank example. A silicon loan officer finds many potential clients want to have their loans paid into their accounts held by the People's Bank of the Third World, which happens to be absent a list of registered banks. The presence of so much business from that quarter (and the ostensible popularity of the bank) suggests that a subtle change in rules is necessary to win loan business. The program deems such an arrangement acceptable. It later turns out these requests have been manufactured. The bank exists but it is a front for illicit arms transfers. Absent the instant

credibility from the misinformed loan officer—more likely, thousands of equally misinformed ones catching the same traffic on the network—it would never have gotten off the ground. Within seconds, the People's Bank has real assets to play with.

Fraud, of course, was not invented for computers (resemblance between this example and a combination of Penn Square and BCCI is not accidental). But computers and networks let far more and far graver mistakes to be made far faster. Error, gossip, and fads can propagate faster than wisdom. Computers also lack the ability to read subtle clues in personal interaction that have guided human decision making for so long. Computers, while immune to certain human faults, are heir, particularly when overconfidently introduced in place of humans, to their own psychoses. Such psychoses can be targeted for exploitation. Systems that learn from and react to each other may exhibit extremely chaotic behavior if ticked in precisely the wrong way.

How dangerous would net warfare be? In some ways, more because bad karma will duplicate itself much faster and farther than in human systems. In other ways, less. Corrective lessons can also propagate faster. Simple safety rules can save lives (e.g., never have traffic lights show green in both directions) even if complex systems are biased towards gridlock and waste under ambiguous conditions (e.g., if in doubt, shut power stations down but keep life-support

equipment on). Security systems can be isolated from external inputs even at the cost of their being harder to work with (e.g., certain computers can be reprogrammed only on site).

So What?

The twentieth century has seen large wars result from the alignment of national communities with the state violence. Millions died when Germans fighting for the Fatherland fought Russians protecting Mother Russia. The Net works against such correlation by making it easier for people to be different, letting them pick and choose among communications flows and thus messages.

The increasing importance of spanning communities over local or national ones may be a harbinger of less war—but not necessarily less violence. True, very dispersed communities, for that reason, cannot easily assemble enough critical mass to take on state power, but, even dispersed, they can do considerable damage. A group turned inward becomes deaf to the message of common discouragement and can potentially more hostile to tenets of civilization. The Net promotes, not insurrection, but greater anomie—in some cases, group anomie—but not necessarily at levels conducive to unconventional conflict.

Wherever this information revolution takes the world, the United States will get to first. It is the only large nation in this century where random internal violence has killed more people than wars. If nothing else, the United States may have worked through the problems of national meaning while they tear at others whose nationhood is based on thin cultural or genetic ice.

As national cultures compete for global influence in this new era, the United States stands to gain most. Our language is most likely to become universal, our currency is in greatest circulation, our social culture remains popular (if poorly understood), and our political culture is likely to continue its ascendancy in world affairs. The United States generates more good information, in terms of science, technology, business, entertainment, and thought than any other single country. The American culture absorbs information (just as we have absorbed people) more readily. Those who mine the world's data basins are more likely to hit our nuggets than hit anyone else's. People everywhere believe that American life is attractive. This is no small factor in favor of our national security, and one that information technology cannot help but widen our lead in.

The tension between vulnerability and service will characterize the prospects for conflict in the Net. If the Net becomes part of our expectations of a good life during benign years before being targeted, dependence

will grow and security will be an afterthought. Attack would lead to great harm. Too much Net security (perhaps resulting from earlier attacks) may keep it from winning acceptance, at the cost of valuable efficiency. Somewhere in between lies a future in which wise security choices and healthy skepticism yield a Net that can ward off most blows, absorb the rest, and maintain its viability.

7 *Conclusions: Mesh Versus Net*

Many of the capabilities that the United States has laboriously constructed to support its Mesh are becoming available to others for fee on the Net. Yet the development of the Net, in general, still favors U.S. security interests.

As long as the power of information technology doubles every two to three years, it will continue to be have a disproportionate effect on the evolution of national security. The emergence of meshes—with their dispersed sensors, emitters, microbots, and miniprojectiles—will drastically hasten the effective retirement of platforms. Thus habits of power based on the differential possession of these items will have to be replaced by habits born of a different calculus.

For the time being, it is difficult to recall a time when the gap between the world's greatest power—which happens to be the United States—and whoever is number two has been so large. To some extent our unipolar superiority has reflected our economic power. If economics were the only cause, however, the nontrivial likelihood that China and Japan could both enjoy national incomes in excess of ours in a decade or two should deservedly given us considerable pause. Fortunately, our superiority is based on more than money; the United States clearly

retains the military capital, infrastructure, institutions, and habits that come with being, by a larger margin, the world's leading military superpower.

Yet all these factors rest, in turn, on our superiority at fielding a platform-based military. If platforms go, would our power advantage follow? Not necessarily. In many ways the United States has an even more impressive lead in information-based warfare, and our relative superiority in software (both technical and cultural) is putatively ours to lose.

As the discussion above, however, suggests, all this has a catch. To wit, the large lead the United States has built up in information warfare has been as a result of a large DOD-financed information infrastructure—the Mesh, to date. Many of the capabilities of this infrastructure, via extension or duplication, will become available to the Net and thus to anyone for far smaller sums then the United States has laid out over the years.

Examples abound, as earlier passages have suggested. DOD put up a fleet of GPS satellites but now anyone can access them by purchasing a GPS receiver. True, DOD has the capability to degrade the signal reaching anyone without the right combinations, but others are developing methods to go around such restrictions (e.g., differential GPS). Many of our space reconnaissance capabilities can be duplicated by anyone with enough money to purchase images from foreign

observation satellites. Thanks to the boom in environmental monitoring, the number of surveillance birds increases by the year. The global internet extends everywhere, permitting any attached country to carry information over borders and in very large quantities. The encryption formerly available only to those with sophisticated computers can be a routine feature of all communications gear within a decade or two. Global cellular communications based on several satellite proposals (e.g., Motorola's Iridium) can be the command and control apparatus of any group that can pay the bills (or have some ostensible neutral pay the bills). The same system used for civilian air traffic control can be adapted to military command and control very easily. When fifty seven (or five hundred) channels becomes ubiquitous from direct broadcast satellites or cellular video, interposing our own video streams in exclusive place of someone else's becomes quite problematic.

The point is not that DOD cannot shut off access to such services. It can, but at a cost which, in political terms, grows more expensive every year. Most of the genies are out of the bottle. Short of a war that puts the survival of the United States or its large allies at risk, DOD will be politically constrained. Yet that is precisely the most probable environment that DOD faces through the next two decades.

In the long run, however, the Net may enhance our national security. The emergence of transnational

communities made possible by the Net should inhibit the dominance of human monocultures in tomorrow's national security environment. Conversely, however, the decline of constraints on human behavior coming from traditional cultures portend a rise in urban anomie which verge on the anarchic.

The future of national security in a time of free silicon is that war becomes peace. Threats of mass destruction will remain difficult to control for precise ends. These aside, those who go outside the law to threaten states succeed precisely to the extent that they play at the margins of security regimes. Like any good disease, they resemble contaminants that the society chooses not to differentiate from legitimate proteins. Societies repel such forces through double filtration. The gross filter determines the proper balance between freedom and ultimate security (as too little freedom is the surest underminer of security). The fine filters finds ever more sophisticated ways to differentiate legitimate users from illegitimate intruders.

Information technology, ironically, restores man to the center of the struggle for national security—where he was before the machines started taking over. Realms of conflict where machines reign supreme—space, air, sea, deserts, and plains (roughly in that order)—will be the first in which the large and complex are brought down by the small and the many. Realms where machines availed little—mountains, forests, jungles, cities, and face-to-face interactions

(again, roughly in that order) are also where the meshes will have smaller and later influence. There, the individual warrior retains the advantage. With unconventional warfare, where warfighting machines are virtually useless, these nets are precisely the point of maximum vulnerability for both sides.

Appendix: Inevitability Detoured

The inevitability and relevance of the Small and the Many may be challenged by several factors: weapons of mass destruction, wide-area electronic counter-measures, the repeated difficulties of making artificial intelligence work, and the simple persistence of legacy warfare systems.

Just in case the future wanders away from these predictions, readers can get a head start on Monday morning by counting, in advance, all the ways it can get lost.

Obstacles to the triumph of the small and the many are numerous. Developments in wholesale war—nuclear, biological, or chemical agents—may obviate any technologies that alter the calculus of retail war. Even in retail war, new technologies usable only in large complex systems might nullify or destroy the small and the many en masse. Much of what lets small chips replace big manned platforms assumes advances in artificial intelligence, whose progress is notoriously resistant to forecast. Old technologies and institutions have ways of fighting back against new technologies that promote confusion; thus, crossover points frequently recede.

The Irrelevance of Retail War: To resolve important issues, would nations worry about the art of grabbing or defending territory or might they instead reach for weapons of mass destruction first?

Weapons of mass destruction come in three types: chemical, biological, and nuclear. Chemical weapons are not likely to affect the dominance of the small and many. Because few chemicals can affect the Mesh, their tactical application is limited. Today's chemicals are just one more obstacle to manned warfare on the battlefield. The low chances of a breakthrough chemical weapon mean the current calculus of uncertain effectiveness and certain retaliation will persist. Hitting U.S. civilian targets requires the use of strategic delivery vehicles. The few who may get them would not waste them on chemical weapons if nuclear ones are available. Successful use invites nuclear retaliation—yielding little scope for chemical weaponry.

Biological weaponry is even harder than chemicals to use tactically. The ability of germs to multiply permits havoc disproportionate to their payload; yet their battlefield use has been rare. Germs are hard to control and may backfire as gas did when first used in World War I. Their effect on humans is extremely difficult to test. The more open the world, the harder it will be to hide errant tests. Greater sophistication could lead to greater disaster. Anthrax, for instance, is very potent, but infected areas are uninhabitable to

friend or foe for eons. Germs that kill their host quickly will not spread quickly. Germs that kill slowly cannot be timed for tactical military advantage. As with chemical weapons, effective germ use may trigger nuclear retaliation.

The strategic use of biological warfare may be more effective but runs the risk that the induced disease crosses national boundaries and comes home. However, a trump card of biological warfare could be the virus that is made genetically specific to target hosts. For instance, a virus that attacks only yams that grow in an enemy country might reduce the latter to starvation. More sinister would be a virus that attacks people of a limited human genotype. It is not clear, however, where any of the zillion combinations of nucleic acids would yield such a virus (much less whether one might be discovered soon).

Would nuclear proliferation make retail war obsolete? During the Cold War, both sides took conventional and nuclear operations seriously. They conducted the former but never the latter thanks to the nuclear stalemate.

The advantage of nuclear weaponry *against* (as opposed to instead of) the small and the many may be that it can destroy or disable the millions without having to look for them. A field swept clean of such objects would let platforms march through, even if just temporarily.

Yet, tactical nuclear weapons (even discounting their potential for escalation to strategic ones) may be no more effective against Meshes than General Grant's use of explosives at the battle of Cold Harbor. Fields cleared by one side may be promptly reseeded by the other with more sensors; the respite in between may be too temporary to yield much advantage. Delivery vehicles for nuclear arms are subject to the same real-time tracking and targeting that conventional platforms are subject to.

Nuclear weapons might also be used to generate an electro-magnetic pulse (EMP) big enough to clear electronics from an area so large that it cannot be reseeded quickly. However, Mesh electronics should be less vulnerable to EMP than are large systems connected to long wires. The only wire associated with such items would be receiving antennae which could be fitted with protective diodes to keep a large induced wave from frying the chips, themselves. Hardening electronics is another possibility. However, if Mesh components diverge to far from their commercial counterparts, they would become too expensive to buy in the right quantities.

Powers in the Big: Might there arise militarily decisive technologies available only in very large sizes that could erode the logic of the Mesh?

EMP effects smaller than those generated by nuclear weapons can be provided by microwave

weapons, for instance. Such weapons require considerable reserves of energy to be effective, but could fry weapons systems electronics at a considerable distance. By staying under the nuclear threshold, microwave weapons may be more usable. Yet if they are less powerful, they would have less effect. They could also be tracked in real time before being used.

Incoming missiles with electronic targeting may be useless if countered by microwaves in certain situations; without missiles all the data generated by the Mesh would avail naught. Yet must missiles be that vulnerable? Those inertially guided and mechanically fuzed, do not need electronics. Moreover, the cost of the microwave machine may be greater than the cost of saturating its defenses with enough not-very-smart rockets to destroy it.

Finally, many sensors may be simply unavailable in small form. In particular, those which require being bathed in very cold liquids to work well may only function if coupled with large expensive cryogenic devices. The latter include SQUIDS (superconducting quantum interference devices) and certain types of infrared detectors (otherwise confused by ambient heat).

Shortfalls in Artificial Intelligence: The hoary "if it works, it isn't artificial intelligence" retains a certain bitter truth after several decades. Both advocates and skeptics of artificial intelligence share a long history of bad predictions. Advocates have consistently

underestimated how much horsepower is required for useful work. Predictions of easy automatic language translation were made in the 1960s but only now can such programs be purchased. Conversely, skeptics predicted that certain feats—a computer beating a grand-master at chess—were inherently impossible, but within the last two years, a computer has defeated a grand-master.

Each of the three relevant areas of artificial intelligence—pattern recognition, machine learning, and synthetic logic—has seen startling successes and dismal failures. For pattern recognition, in particular, the trend is away from linear logical approaches and toward imitating human neural techniques. The excitement that greeted the widespread introduction of neural net techniques in the mid-1980s has abated—functional nodal architectures are more complex than first realized. On the other hand, companies are busy casting neural net chips, so there must be something there.

Broad analogues of the human brain—notably the faculty of common sense—are still eons away. The more limited a domain (e.g., if all dialogue concerns biochemistry), the faster the chances for success. Ironically, the persistence of domain limitation argues against robotic images of technology and toward complex networks of simple sensors. But it still leaves man as integral to command and control in warfighting.

The Persistence of Legacy Systems: The last barrier to the Mesh is that radical futures seem to take longer getting here than simple technological extrapolation would suggest. Picking broad trends is easy; solving the thousands of problems that must be faced before the broad trends are realized is not.

The new always faces the resistance of the old, aided by patterns of familiarity, sunk costs, well-tested habits, and a large supportive infrastructure—hence the observation that a the new must improve over the old by a factor of ten if it is to overtake it. In the meantime, the old rarely stands still. Chips are still made with silicon even the same chips recast in gallium arsenide would run three to five times faster. Silicon technology has been pushed past hitherto disabling hurdles, even as the promise of gallium arsenide confronts problems not clearly understood at the outset.

Yet: Two major considerations still favor the Mesh. First, the commercial technologies continue to advance; as they do, the gap between existing military systems and new systems based on commercial components shrinks. Advanced economies that have yet to develop a large military-industrial complex (e.g., Japan or the collectivity of overseas Chinese) would find that this gap could be bridged quickly. The route to a superior military, which otherwise would retrace the path taken by other nations, could be shortened by flying through a technological worm-hole.

Second, military technology continues to be intensely competitive, thus success in one place would promote its spread elsewhere. True, an agreement among superpowers can suppress *known* lines of development. Arms control and non-proliferation treaties have worked. Used to suppress a *speculative* line of development in an era of great strategic uncertainty, however, their success is less certain.